

# MAKING THE INTERNET SAFE FOR KIDS: THE ROLE OF ISP'S AND SOCIAL NETWORKING SITES

---

## HEARINGS BEFORE THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS  
SECOND SESSION

JUNE 27 AND JUNE 28, 2006

**Serial No. 109-123**

Printed for the use of the Committee on Energy and Commerce



Available via the World Wide Web: <http://www.access.gpo.gov/congress/house>

U.S. GOVERNMENT PRINTING OFFICE

30-530PDF

WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas	JOHN D. DINGELL, Michigan
MICHAEL BILIRAKIS, Florida	<i>Ranking Member</i>
<i>Vice Chairman</i>	HENRY A. WAXMAN, California
FRED UPTON, Michigan	EDWARD J. MARKEY, Massachusetts
CLIFF STEARNS, Florida	RICK BOUCHER, Virginia
PAUL E. GILLMOR, Ohio	EDOLPHUS TOWNS, New York
NATHAN DEAL, Georgia	FRANK PALLONE, JR., New Jersey
ED WHITFIELD, Kentucky	SHERROD BROWN, Ohio
CHARLIE NORWOOD, Georgia	BART GORDON, Tennessee
BARBARA CUBIN, Wyoming	BOBBY L. RUSH, Illinois
JOHN SHIMKUS, Illinois	ANNA G. ESHOO, California
HEATHER WILSON, New Mexico	BART STUPAK, Michigan
JOHN B. SHADEGG, Arizona	ELIOT L. ENGEL, New York
CHARLES W. "CHIP" PICKERING, Mississippi	ALBERT R. WYNN, Maryland
<i>Vice Chairman</i>	GENE GREEN, Texas
VITO FOSSELLA, New York	TED STRICKLAND, Ohio
ROY BLUNT, Missouri	DIANA DEGETTE, Colorado
STEVE BUYER, Indiana	LOIS CAPPS, California
GEORGE RADANOVICH, California	MIKE DOYLE, Pennsylvania
CHARLES F. BASS, New Hampshire	TOM ALLEN, Maine
JOSEPH R. PITTS, Pennsylvania	JIM DAVIS, Florida
MARY BONO, California	JAN SCHAKOWSKY, Illinois
GREG WALDEN, Oregon	HILDA L. SOLIS, California
LEE TERRY, Nebraska	CHARLES A. GONZALEZ, Texas
MIKE FERGUSON, New Jersey	JAY INSLEE, Washington
MIKE ROGERS, Michigan	TAMMY BALDWIN, Wisconsin
C.L. "BUTCH" OTTER, Idaho	MIKE ROSS, Arkansas
SUE MYRICK, North Carolina	
JOHN SULLIVAN, Oklahoma	
TIM MURPHY, Pennsylvania	
MICHAEL C. BURGESS, Texas	
MARSHA BLACKBURN, Tennessee	

BUD ALBRIGHT, *Staff Director*

DAVID CAVICKE, *General Counsel*

REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

ED WHITFIELD, Kentucky, *Chairman*

CLIFF STEARNS, Florida	BART STUPAK, Michigan
CHARLES W. "CHIP" PICKERING, Mississippi	<i>Ranking Member</i>
CHARLES F. BASS, New Hampshire	DIANA DEGETTE, Colorado
GREG WALDEN, Oregon	JAN SCHAKOWSKY, Illinois
MIKE FERGUSON, New Jersey	JAY INSLEE, Washington
MICHAEL C. BURGESS, Texas	TAMMY BALDWIN, Wisconsin
MARSHA BLACKBURN, Tennessee	HENRY A. WAXMAN, California
JOE BARTON, Texas	JOHN D. DINGELL, Michigan
<i>(EX OFFICIO)</i>	<i>(EX OFFICIO)</i>

# CONTENTS

---

	Page
Hearings held:	
June 27, 2006.....	1
June 28, 2006.....	178
Testimony of:	
Hansen, Chris, NBC News.....	20
Ryan, John, Esq., Chief Counsel, Compliance and Investigation, America Online, Inc. ..	49
Baker, Dave, Vice President, Law and Public Policy, Earthlink, Inc. ....	58
Banker, Elizabeth, Associate General Counsel, Yahoo! Inc. ....	79
Dailey, Tom, General Counsel, Verizon Communications.....	90
Lewis, Jr., Gerald J., Vice President, Deputy General Counsel & Chief Privacy Officer, Comcast Cable Communications .....	98
Reitinger, Philip R., Senior Security Strategist, Microsoft Corporation.....	122
Wong, Nicole, Associate General Counsel & Chief Privacy Officer, Google, Inc.....	139
Dannahey, Frank, Detective, Rocky Hill, Connecticut Police Department .....	191
Kelly, Chris, Vice President, Corporate Development and Chief Privacy Officer, Facebook.com, Inc. ....	214
Angus, Michael, Executive Vice President and General Counsel, Fox Interactive Media, MySpace.com.....	218
Hiller, John, Chief Executive Officer, Xanga.com, Inc.....	249
Harbour, Hon. Pamela Jones, Commissioner, Federal Trade Commission .....	289
Ruiz, Diego, Office of Strategic Planning and Policy Analysis, Federal Communications Commission .....	297
Blumenthal, Hon. Richard, Attorney General, State of Connecticut .....	304





# **MAKING THE INTERNET SAFE FOR KIDS: THE ROLE OF ISP'S AND SOCIAL NETWORKING SITES**

---

**TUESDAY, JUNE 27, 2006**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ENERGY AND COMMERCE,  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10:07 a.m., in Room 2123 of the Rayburn House Office Building, Hon. Ed Whitfield (Chairman) presiding.

Members present: Representatives Whitfield, Stearns, Pickering, Bass, Walden, Ferguson, Burgess, Blackburn, Barton (ex officio), Stupak, DeGette, Schakowsky, Inslee, and Baldwin.

Staff present: Mark Paoletta, Chief Counsel for Oversight and Investigations; Alan Slobodin, Deputy Chief Counsel for Oversight and Investigation; Karen Christian, Counsel; Kelly Andrews, Counsel; John Halliwell, Policy Coordinator, Mike Abraham, Legislative Clerk; Ryan Ambrose, Legislative Clerk; David Nelson, Minority Investigator/Economist; and Elizabeth Ertel, Minority Staff Assistant.

MR. WHITFIELD. This hearing will come to order.

And I want to thank the panel of witnesses for taking time from their busy schedules to be with us today.

Today, we are holding the first day of a 2-day hearing entitled: "Making the Internet Safe for Kids: The Role of Internet Service Providers and Social Networking Sites".

Our previous hearings explored issues relating to the sexual exploitation of children over the Internet. Those hearings made it apparent that we have a long way to go in making the Internet a safe place for our children. We heard wrenching testimony from two child victims of Internet predators, Justin Berry and Masha Allen. Their stories brought to life the horrors that can occur on the Internet to children. We also heard law enforcement agency representatives express their concern about the staggering number of children and child predators and pedophiles on the Internet today.

The Internet has created what one of our witnesses called a "virtual Sears catalog" for pedophiles to find and communicate with children,

because the Internet has become, as you all know, a social gathering place for children.

We must minimize the likelihood of our children being exploited over the Internet, and we must do everything possible to assist law enforcement in their efforts to investigate and prosecute child predators.

I want to thank our first panel witness, Mr. Chris Hansen, from Dateline NBC for testifying today about his riveting investigative series called "To Catch a Predator". This series showed how child predators in five different cities across America chatted with someone over the Internet that they believed to be a 13- or 14-year-old child and then actually travel to a home to meet this supposed child for sexual activity.

Mr. Hansen pointed out very clearly, and I think we will talk about it today, how predators come from all walks of life and are all different ages and backgrounds. And it is difficult to predict who really is a child predator. There certainly does not appear to be any profile of who over the Internet may be a child predator. This is particularly important for parents and children to understand, and I look forward to hearing more from Mr. Hansen about his investigative work in this series.

I want to thank also the representatives of the Internet service providers who are here today. We look forward to their testimony explaining what they are doing to assist law enforcement in cases involving this sexual exploitation of children over the Internet and what measures the companies are taking to minimize opportunities to sexually exploit children from their networks.

We certainly understand that Internet service providers are not law enforcement agencies, and I certainly am not asking them to become that. I do believe that having images or links to images that may be child pornography are, at a minimum, violations of their terms of use and may be criminal sites as well.

Taking measures to proactively look for this content on your network, reporting this content to the National Center for Missing and Exploited Children and to law enforcement will go a long way towards reducing access that pedophiles have websites with sexually exploitive images of children. If companies have concerns about performing proactive searches of this content, we hope you will express that today. This would be the appropriate time to talk about your concerns if you think it produces a burden on your company. I understand that several companies have undertaken proactive searching and filtering of these sites and images, and we look forward to hearing about that in their testimony today.

I am also interested in learning about the Internet service providers' data retention policies for IP addresses in particular. A witness at this subcommittee's prior hearing, Flint Waters, testified that in connection to

an investigation about a child predator on the Internet, he was unable to get subscriber information for a 3-day old IP address from an Internet service provider. That is unacceptable. Law enforcement agency representatives have testified that retaining these IP addresses is critical to their being able to catch these people.

I understand that several companies today and tomorrow will make announcements about ways they are enhancing their networks to help combat the exploitation of children on their networks, whether it is increasing the length of time they retain the IP address, enhancing their filtering devices, or providing additional safety measures for parents and children to employ on their network. I commend all of those efforts, and we look forward to hearing more about it this morning.

We have a simple message: let us make it as difficult as possible for child predators and pedophiles to trade images, set up illegal websites, and find children on the Internet.

[The prepared statement of Hon. Ed Whitfield follows:]

PREPARED STATEMENT OF THE HON. ED WHITFIELD, CHAIRMAN, SUBCOMMITTEE ON  
OVERSIGHT AND INVESTIGATIONS

TODAY WE ARE HOLDING THE FIRST DAY OF A TWO-DAY HEARING ENTITLED "MAKING THE INTERNET SAFE FOR KIDS: THE ROLE OF ISP'S AND SOCIAL NETWORKING SITES." OUR PREVIOUS HEARINGS EXPLORED ISSUES RELATING TO THE SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET. THOSE HEARINGS MADE IT APPARENT THAT WE HAVE A LONG WAY TO GO IN MAKING THE INTERNET A SAFE PLACE FOR OUR CHILDREN. WE HEARD WRENCHING TESTIMONY FROM TWO CHILD-VICTIMS OF INTERNET PREDATORS—JUSTIN BERRY AND MASHA ALLEN. THEIR STORIES BROUGHT TO LIFE THE HORRORS THAT CAN OCCUR ON THE INTERNET TO CHILDREN. WE ALSO HEARD LAW ENFORCEMENT AGENCY REPRESENTATIVES EXPRESS SHOCK ABOUT THE STAGGERING NUMBER OF CHILD PREDATORS AND PEDOPHILES ON THE INTERNET. THE INTERNET HAS CREATED WHAT ONE OF OUR WITNESSES CALLED "A VIRTUAL SEARS CATALOG" FOR PEDOPHILES TO FIND AND COMMUNICATE WITH CHILDREN BECAUSE THE INTERNET IS BECOMING THE SOCIAL NETWORKING PLACE FOR YOUNG PEOPLE.

WE MUST MINIMIZE THE LIKELIHOOD OF OUR CHILDREN BEING EXPLOITED OVER THE INTERNET AND TO EVERYTHING POSSIBLE TO ASSIST LAW ENFORCEMENT IN THEIR EFFORTS TO INVESTIGATE AND PROSECUTE CHILD PREDATORS.

I WANT TO THANK OUR FIRST PANEL WITNESS, MR. CHRIS HANSEN, FROM DATELINE NBC FOR TESTIFYING TODAY ABOUT HIS RIVETING INVESTIGATIVE SERIES CALLED "TO CATCH A PREDATOR." THIS SERIES SHOWED HOW CHILD PREDATORS IN FIVE DIFFERENT CITIES ACROSS AMERICA, CHATTED WITH SOMEONE OVER THE INTERNET THEY BELIEVED TO BE A 13 OR 14 YEAR OLD CHILD AND THEN ACTUALLY TRAVELLED TO A HOME TO MEET THE CHILD FOR SEXUAL ACTIVITY. WHAT I FOUND MOST TELLING FROM WATCHING SOME OF THE EPISODES IS THAT THESE CHILD PREDATORS COME FROM ALL WALKS OF LIFE AND

ARE ALL DIFFERENT AGES AND BACKGROUNDS. THERE DOESN'T APPEAR TO BE ANY PROFILE OF WHO—OVER THE INTERNET—MAY BE A CHILD PREDATOR. THIS IS IMPORTANT FOR PARENTS AND CHILDREN TO UNDERSTAND. I LOOK FORWARD TO HEARING MORE FROM MR. HANSEN ON HIS INVESTIGATIVE WORK IN THIS SERIES.

I WANT TO THANK THE REPRESENTATIVES OF THE INTERNET SERVICE PROVIDERS WHO ARE HERE TODAY. WE LOOK FORWARD TO THEIR TESTIMONY EXPLAINING WHAT THEY ARE DOING TO ASSIST LAW ENFORCEMENT IN CASES INVOLVING THE SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET AND WHAT MEASURES THE COMPANIES ARE TAKING TO REMOVE IMAGES, WEBSITES AND OTHER ILLEGAL CONTENT THAT SEXUALLY EXPLOIT CHILDREN FROM THEIR NETWORKS. INTERNET SERVICE PROVIDERS ARE NOT LAW ENFORCEMENT AGENTS--- AND I CERTAINLY AM NOT ASKING THEM TO BECOME THAT—I DO BELIEVE THAT HAVING IMAGES OR LINKS TO IMAGES THAT MAY BE CHILD PORNOGRAPHY ARE, AT A MINIMUM, VIOLATIONS OF THEIR TERMS OF USE AND MAY BE CRIMINAL SITES AS WELL. TAKING MEASURES TO PROACTIVELY LOOK FOR THIS CONTENT ON YOUR NETWORK, REPORT THIS CONTENT TO THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN AND TO LAW ENFORCEMENT, WILL GO A LONG WAY TOWARDS REDUCING ACCESS THAT PEDOPHILES HAVE WEBSITES WITH SEXUALLY EXPLOITATIVE IMAGES OF CHILDREN. IF COMPANIES HAVE CONCERNS ABOUT PERFORMING PRO-ACTIVE SEARCHES OF THIS HORRIFIC CONTENT— WE HOPE YOU WILL EXPRESS THEM TODAY. I UNDERSTAND THAT SEVERAL COMPANIES HAVE UNDERTAKEN PROACTIVE SEARCHING AND FILTERING OF THESE SITES AND IMAGES—AND ARE LOOKING FORWARD TO THAT TESTIMONY.

I ALSO AM INTERESTED IN LEARNING ABOUT THE INTERNET SERVICE PROVIDERS DATA RETENTION POLICIES FOR IP ADDRESSES IN PARTICULAR. A WITNESS AT THE SUBCOMMITTEE'S PRIOR HEARING—FLINT WATERS--TESTIFIED THAT IN CONNECTION TO AN INVESTIGATION ABOUT A CHILD PREDATOR ON THE INTERNET, HE WAS UNABLE TO GET SUBSCRIBER INFORMATION FOR A THREE-DAY OLD IP ADDRESS FROM AN INTERNET SERVICE PROVIDER. THIS IS UNACCEPTABLE. LAW ENFORCEMENT AGENCY REPRESENTATIVES HAVE TESTIFIED THAT RETAINING IP ADDRESSES IS CRITICAL.

I HAVE A SIMPLE MESSAGE: LET'S MAKE IT AS DIFFICULT AS POSSIBLE FOR CHILD PREDATORS AND PEDOPHILES TO TRADE IMAGES, SET-UP ILLEGAL WEBSITES AND FIND CHILDREN ON THE INTERNET.

MR. WHITFIELD. At this time, I recognize the distinguished Ranking Member, Mr. Stupak of Michigan.

MR. STUPAK. Thank you, Mr. Chairman, and thank you for calling this hearing, and thank you for continuing to do this investigation in a bipartisan manner.

A growing scourge of what is called "child pornography and exploitation" on the Internet is a serious threat to all of our children. I say so because what this really involves is the rape and torture of children for profit or to satisfy some dark urges. It was a well-contained problem before the advent of the Internet. The anonymity of the Net has

apparently brought out the worst in a small but growing number of Americans and allowed them to communicate with their counterparts all over the world.

The statistics are startling. Eighty percent of the pornographic images of children on the Net involve children ages 12 and under. Forty percent involve children ages 6 and under. Twenty percent involve toddlers ages 3 and under.

The National Center for Missing and Exploited Children estimates that 40 percent of those that view child pornography have or will abuse their own children. We have had testimony that preliminary information from studies, soon to be published, that number may actually rise to 75 to 80 percent. People that think viewing these images is a victimless crime simply do not understand the problem.

There is both good news and bad news. The bad news is that our children are at a substantial and growing risk. The good news is that if these predators can be denied easy access to the images that provoke them and if we can make it risky for them to groom young victims, we can, once again, make this dangerous behavior rare.

This will require the best efforts of all of us. Yes, we need to find effective ways to educate parents and children about the dangers of putting personal information out on the Net. Yes, we need to greatly expand the resources available to State, local, and Federal law enforcement agencies. Yes, we must make it clear to prosecutors that cutting deals for minimal jail time and/or probation is unacceptable for these men that terrorize our children and those that are caught "only enjoying the images" of these heinous acts. And yes, we must let judges know that they may no longer endanger society by releasing these criminals with a slap on the wrist.

As Members of Congress, we have a unique responsibility not only to ensure that Federal criminal laws are adequate and that Federal law enforcement is up to snuff, but also to deny access to the Internet of those that hunt our children and profit from the sale of these awful images.

Mr. Chairman, I am glad to see Mr. Chris Hansen here today whose Dateline NBC series on child predators has awakened America to the dangers our children face. This series of programs has shown us exactly what lengths these men from all walks of life are willing to go to to abuse children.

Testimony to date has revealed the following statistics: 50,000 predators are online at any given time; 1 in 5 children will be solicited online; 1 in 33 of these solicitations, just about the size of an overcrowded classroom, will result in the successful contact of a child by phone, letter, or physical meeting. I suspect that what Mr. Hansen has to

tell us will provide important context for the examining of the testimony of the social networking websites that will appear before us tomorrow.

I am also pleased that you have assembled seven Internet service providers to testify today. Certainly it is important for us to know the extent to which some ISPs have made to combat children pornography on their sites. Some ISPs have cooperated with law enforcement and are proactively attempting to eliminate child pornography from their networks while others seem to be in denial that they have children being abused over their networks.

But make no mistake about it, regardless of the level of effort expended so far, it is not enough. The problem is growing. Mr. Chairman, we have gathered witnesses that can provide some information, and some will be making very important announcements today. However, absent are the CEOs who can make the voluntary commitments of the resources and cooperation necessary to clean up the Web.

Voluntary action in the United Kingdom has made great strides in limiting the commercial use of the World Wide Web in that country to sell or view child porn. When these efforts began approximately 3 years ago, the UK hosted 18 percent of the commercial child porn sites worldwide. Today, that number is down to four-tenths of one percent. It is estimated that the United States hosts 42 percent of the worldwide for-profit sites. Since 2000, the CyberTipline operated by the National Center for Missing and Exploited Children has seen reports of these gruesome images grow from 20,000 to over 390,000 today.

I would like to see our Internet and telecom companies commit to taking down every identified site in the United States and blocking the American predators from using U.S.-based network platforms to access child pornography from any identified site worldwide.

As the author of an amendment to the House Telecommunications Bill to require broadband carriers to prevent child pornography from traveling on their networks, I am very interested in knowing the ISPs' reaction to this idea. I also want to know if they will support tougher data retention policies for parent and known child pornography. Will this solve the problem? No, but it will make a substantial dent in the multi-billion-dollar industry that seeks to exploit children for profit. It will reduce the demand that drives much of the exploitation and will save many children from this terrible abuse.

With that, Mr. Chairman, I yield back the balance of my time.

MR. WHITFIELD. Thank you, Mr. Stupak.

At this time, I recognize the Vice Chairman of this committee, Mr. Walden of Oregon.

MR. WALDEN. Thank you very much, Mr. Chairman. I commend you for holding this hearing as we continue to investigate this terrible scourge that is on our population.

I want to congratulate Chris for the work he has done at NBC to really shine light for the whole country to see just how awful this is and how pervasive it is. I think most parents don't have a clue that this could be going on in their own family room where a kid is hooked up to a computer, and yet we know, from our work on this committee, and you have identified from the work you have done, it is very easy to get caught up in the web of predators and perverts in this country who seek out children to do ghastly things to them. And so I commend you for that work, and I appreciate it as a parent. It has been most troubling to learn about what does go on out there, and I think most parents in America would share that, that they just can't believe this happens and how easily and quickly it happens. I think one of the most disturbing things, Mr. Chairman, I have come to understand out of our hearings is within seconds, you can identify a predator online or they can identify you. And the grooming process begins, the manipulation begins, and the horror begins. And we have had witnesses before this subcommittee who have told us their stories and told America their stories, and hopefully, we will all learn from that.

I am pleased to see that the industry is responding in the way it should respond with the announcements today of their work that they are going to do with the National Center for Missing and Exploited Children to develop both technological solutions as well as better enforcement tools and enhance their industry efforts. But I dare say there is more work to be done in terms of who is able to link to what site and who gets paid for that and how we filter that out. Some ISPs are better than others at that. And so our work continues.

But Mr. Chairman, I think the work of this committee and the work of journalists like Mr. Hansen come a long way toward exposing the problem, and frankly, shining light on a problem as horrific as this one is is a good first step and a good tonic. There are other things we can do legally, and there are certainly things the industries can do collaboratively to do everything we can to protect our kids and to clean up the Internet.

With that, Mr. Chairman, I yield back the balance of my time.

MR. WHITFIELD. Thank you.

At this time, I will recognize Ms. DeGette of Colorado.

MS. DEGETTE. Thank you very much, Mr. Chairman, for tackling this series of hearings on a very important subject.

I have been amazed in these hearings, and as the mother of two girls ages 16 and 12, I have been scared about the data that we are hearing,

because child pornography on the Internet is burgeoning. It is exploding out of control, and it is time for everybody involved in our society to take this seriously and to look at some serious steps to controlling it.

Only one percent of the images on the Internet are just simply nudity. This is very serious exploitation of children, and I am not going to go into the graphic details. Suffice it to say it is appalling, and it is easy to pull up on your computer.

I will also say, as Mr. Stupak noted, that the number of complaints that people are getting is burgeoning as well. The Department of Justice Internet Crimes Against Children Task Force, in 2003, 3,700 reports of Internet crimes against children. In fiscal year 2005, it went up to 198,000. So we really do need to get a grip on it, and we all need to do it together: the media, Members of Congress, and the providers.

And so, Mr. Chairman, sometimes we wonder if we do any good up here, but the fact that the ISPs are making some announcement of changes of policies today, I think that is based directly on the work of people like Mr. Hansen to bring this out and people like Paula Woodward in Denver at our NBC affiliate who has been working on this. I also think it is a result of these hearings. And I think it is commendable. I am eager to hear these announcements, and I am glad they are doing it, but I still think we need to do more.

And as probably almost everybody in this room knows, and everybody on this committee knows, ever since our first hearing, I started working on legislation that would require companies that provide broadband service to keep certain records that identify their customers for 1 year. Amazingly, even though we require telephone companies to keep records of every telephone call for 18 months so that law enforcement authorities can subpoena those records, there is no Federal law for Internet communications, and there is no industry standard.

As we have heard over and over in our testimony, this is hindering investigations, because when investigators want to go and get evidence, subpoena evidence that they can find these terrible criminal perpetrators, they find that the Internet service information has been destroyed. And so, Mr. Chairman, I have been working with you and your staff and also with Chairman Barton and his staff to make sure that the legislation is drafted so that it protects consumers' rights to privacy. But I have said it before, and I will say it again, I don't think that people who are raping 2-year-old children on the Internet have any right to privacy, and nobody thinks that.

So we need to make our laws work. We need to make our laws work to have people retain records so that they can be subpoenaed in criminal investigations.



Let me just say one thing. I am not saying that the Internet communications should be preserved. And that has been a misunderstanding that has been out there. I am saying that certain identifying information that is readily available and is kept now by Internet service providers should be kept for a period of time so that law enforcement authorities can subpoena that information if they need it in an ongoing investigation.

I think that eradicating this pernicious practice is going to take a national and even a global partnership of citizens, parents, government, industry, and law enforcement. Every single one of us needs to be thinking about how we can do more. Every single parent in this country needs to be thinking about talking to their children about these Internet predators and how they can avoid being victims. And once we do that, just like we eradicated a lot of the child pornography in the mail in the 1980s, I believe that we can rid our computers and our children of this scourge.

Thank you very much, Mr. Chairman, and I yield back.

MR. WHITFIELD. Thank you.

At this time, I recognize Mr. Ferguson of New Jersey.

MR. FERGUSON. Thank you, Mr. Chairman, for holding another hearing on this subject that our committee has brought to the public's attention over the course of the last few months. I am thankful that our committee has made a commitment to educate the public and the Government about a topic which really needs a lot of our attention.

I would also like to thank our witnesses for joining us today and testifying. The witnesses that are coming before the committee today have all made a commitment to bring this issue to light and helping working to protect our children who use the Internet, and for that, we are all very appreciative.

I also want to thank Chris Hansen for being here with us today and taking time to be here. There is no doubt that the "To Catch a Predator" series that recently aired on Dateline NBC came as a shock to all of us who were watching. Perhaps what was most shocking was the wide demographic of men who came with the intention of taking advantage of these children. Throughout the past few months, we learned that there is truly no pattern, profile, or overarching characteristic of these folks. They come from all walks of life, all professions, backgrounds, and education levels, and perhaps that is what is most frightening of all.

I want to thank Mr. Hansen again, and I am anxious to hear what he has to say today about his work with Dateline NBC.

I appreciate the chance to hear from the Internet representatives who are here with us today and what they are doing to stop the flow of child pornography and aid law enforcement in these types of investigations.

There is no doubt that the technology to apprehend these predators has greatly advanced over recent years, and Internet services can be a tremendous resource for law enforcement in these types of crimes.

While we struggle with privacy issues regarding e-mail and Internet chat rooms involved in these cyber crimes, I look forward to finding solutions to this problem. Whatever privacy concerns are out there, we must make sure that we are doing everything we can to protect our children.

Although as Members of Congress, we have done right in bringing this issue to surface, and law enforcement and those in the Internet industry have taken great strides in making efforts to root out predators, there is always more that can be done.

I look forward to working with these groups to further enhance the safety of the Internet while still allowing our children to use it for the many benefits that it can provide. I am also looking forward to hearing from law enforcement and others who work in this area in what is being done in my home State of New Jersey regarding this issue. Our O&I Subcommittee will have a field hearing on July 10 in my district in New Jersey. I want to extend my early appreciation to our U.S. Attorney in New Jersey, Chris Christie, who has already agreed to testify at that hearing.

Again, thank you, Mr. Chairman, for your commitment to these hearings and this issue.

And again, thanks to our witnesses for being here today.

I yield back.

MR. WHITFIELD. Ms. Baldwin of Wisconsin.

MS. BALDWIN. Thank you, Mr. Chairman. And I want to commend you, Mr. Chairman, and this subcommittee's work in prior sessions examining the proliferation of child exploitation over the Internet and its efforts to shed light on the abhorrent but burgeoning networks of child predators online as well as its efforts to educate the public and especially parents about the danger such individuals pose to children who use the Internet.

I, too, want to extend my welcome to Mr. Hansen to today's hearing. Your investigative series "To Catch a Predator" provides startling revelations of just how easy it is for a child predator to initiate online contact with underage persons, how there is no easy way to profile a child predator, and how persistent such predators are in looking for child victims despite high-profile sting operations such as those featured on your program.

Perhaps it helps explain the staggering statistic that one in five children is solicited for sex while online. Your program helps parents understand just how crucial it is for them to be involved with their

children's online activities and to proactively use filtering technologies and safety settings provided by the Internet service providers.

I also appreciate the participation of various ISPs and search engines on the second panel in today's hearing. In reviewing the testimony provided for today's hearing, it is clear to me that different ISPs adopt very different policies in regard to how proactively and aggressively each filters child pornography on its networks as well as its policies of data retention, specifically the length in which IP address assignment and customer record information are retained.

I strongly believe that there ought to be national uniformity in this regard so users of ISPs, especially children, are guaranteed a certain level of protection and that law enforcement officers across the country are assured that their hard work chasing down child predators will not be undermined at the last minute by inadequate data preservation.

I note that several panelists in our second panel have suggested various legislative options in their testimony today, and I look forward to working with members of this subcommittee to produce legislation that will address the needs of law enforcement in investigating and prosecuting child pornography cases while balancing a consumer's right to privacy.

Finally, I have serious concerns regarding the adequacy of the effort of some of the search engines and what they are devoting to monitor and filter child pornography. For example, on our desks here today, are the results of a Google search which uncovered sponsored links hosted by an advertiser with Google on Google's website that purports to market child pornography. I hope that Google can fully explain its "Ad words" service that allows any potential advertiser to create and control their advertisement through an online program. It is clear to me that such a self-managed advertising program requires a substantial amount of resources on the part of Google to screen and enforce its policy prohibiting the promotion of child pornography. And I am doubtful that current efforts are adequate.

In addition, I hope that both Google and Yahoo! will address the issue of online bulletin boards or groups hosted by their websites that allow the exchange of sexually explicit images and material among group members. I am interested in any proactive efforts by Yahoo! and Google to monitor such bulletin boards for their trafficking and exchange of child pornography.

And I hope that this series of hearings will help lead to a reduction of such violent and heinous crimes against children, whether it is through informing parents of the dangers of online child predators, a greater oversight of Federal response to the issue of child exploitation on the Internet, or new legislative proposals that would deter online pedophilia.

Again, I want to thank the subcommittee and Mr. Chairman, Mr. Ranking Member for holding this important series of hearings, and I look forward to the testimony today.

MR. WHITFIELD. Thank you.

Dr. Burgess, you are recognized for your opening statement.

MR. BURGESS. Thank you, Mr. Chairman, and I want to join other members of our committee in welcoming Mr. Hansen here this morning and thank him for his groundbreaking work in this field.

Mr. Chairman, we have started this series of intensive investigations on sexual exploitation of children over the Internet, and we have heard from a range of parties: courageous child victims, journalists who bring stories to light, law enforcement agencies charged with prosecuting these predators. After each hearing, you can't help but be troubled by what you have learned, and I am proud, Mr. Chairman, that this committee has taken the leadership role in dedicating itself to educating Congress and the public on this most dangerous situation.

As a father of three, I am unable to comprehend how people can commit these types of crimes against children. However, it is crucial, for the safety of our children, for all of us to know about these evils so that we can help curb this abusive practice.

Mr. Chairman, thank you for your leadership regarding this troubling but imperative topic. It is my understanding that after our last subcommittee hearing, Attorney General Gonzales announced that the Department of Justice, in conjunction with various Internet service providers, would study uniform data retention policies for IP addresses. Hopefully, this will enhance the effectiveness of law enforcements' investigations for persons engaged in crimes against children. While some of the providers, like EarthLink, retain data for 7 years, others retain the IPs for as little as 31 days.

In light of the situation, my opinion, retaining this crucial data for only a month is, in itself, almost criminal.

I look forward to hearing from each of the Internet service providers today regarding their own current policies. I also think it would be useful to discuss some of the problems associated with a long period of data retention of these addresses. I believe that the providers have a responsibility to the public, and it will be extremely useful to know what type of safety features and filtering devices each company utilizes to help protect our children.

Further, it is my understanding that we may receive some new information today about new industry standards and new industry practice, and I look forward to learning that information today as well.

While the providers are an important component to this problem, the Government also has a vital role to play. During our last hearing, we

heard how the Government let a young orphan from Russian, Masha Allen, be adopted by a single man, who, in turn, turned out to be a pedophile. There were all types of blatant clues that the Government ignored, including the fact that Masha would not have her own bedroom in this man's home.

Mr. Chairman, how hard was that for the State Department that investigated this man for the suitability of being an adoptive parent, a single father, to ask: "Where is the little girl's bedroom?"

Mr. Chairman, I look forward to us having the State Department back here before this committee to help us answer some of these questions, because the problems that we address in this country, as grievous and as troublesome as they are, pale in comparison to plucking a child out of an orphanage overseas and depositing her into that type of an environment.

As lawmakers, it is our job to create effective laws to keep children away from harm. While at times this is an almost impossible task, we have a responsibility to children and parents to diligently undertake this charge. We must not stop until we fulfill this important obligation to our most innocent and vulnerable segment of society.

Mr. Chairman, thank you, again, for your continued leadership and dedication to this grave situation. I look forward to working with you and others on this committee as we continue to find solutions to this most troublesome problem.

I yield back.

MR. WHITFIELD. Thank you, Dr. Burgess.

I might also add that we intend to bring in some of the adoption agencies as well that were involved in that.

At this time, I recognize the gentleman from Florida, Mr. Stearns.

MR. STEARNS. Thank you, Mr. Chairman.

This, obviously, is a very troubling hearing that we are having here. You would think with the advent of the Internet it would bring a lot of positive things, but obviously this is not a positive thing we are talking about today.

One in five children receives a sexual solicitation while on the Internet, and most never tell an adult. Between 2000 and 2004, Federal criminal referrals of sexual exploitation over the Internet increased by 124 percent. The National Center for Missing and Exploited Children's CyberTipline reported it received more than 100,000 complaints a year regarding online child pornography. On March 15, Julie Myers, Chief of U.S. Immigration and Custom Enforcement, said in a press conference: "Tragically and frighteningly, the kids in these images are getting younger, and the images are getting more and more violent and graphic."

In former hearings, we learned through the disturbing testimony from Mr. Justin Berry, a former victim of child predators, and Mr. Kurt Eichenwald, a reporter for the New York Times, that in this underground predator hunt for children on a legitimate site used by webcam owners and compare strategies and techniques. They simply compare strategies and techniques for luring children into this sordid world.

Pedophiles were all isolated from society and each other in the past, but no longer. The Internet creates a virtual community in which predators reinforce their sick desires. Online portal that advertises for paid webcam child pornography, there are 585 sites. Even after the children shut down these websites, the images remain and are traded online long afterwards.

We have heard about one website claiming to have 140,000 images of adolescents from their webcam.

My colleagues, it is illegal to manufacture and distribute child pornography whether in print form or online, and yet child pornographers produce images without fear or consequences. They are computer-savvy individuals, obviously, whose adaptive skills often outpace law enforcements' ability to simply pursue them.

We need to strengthen our technological capabilities to track down and prosecute these criminals and instill such fear in them of capture and prosecution that they will not harm our children again.

It is also our duty to educate the adults, including all of the mothers and fathers, and to urge them to have close supervision. It is our duty, as Members of Congress, to do whatever we can in our power here this morning to protect the innocent. And certainly a hearing of this nature does help to inform others about this very serious offense.

So I am hoping the testimony will give us a greater insight into what efforts are currently being used to track down these criminals, perhaps also stimulating ideas for reform, either through legislative means or to tighten and enact more law enforcement.

And I thank you, Mr. Chairman.

MR. WHITFIELD. At this time, I will recognize Mr. Inslee of Washington.

MR. INSLEE. Thank you.

I just want to thank Mr. Hansen for your work in this regard. You have helped move Congress. Thank you.

I look forward to your testimony.

MR. WHITFIELD. Mrs. Blackburn of Tennessee.

MRS. BLACKBURN. Thank you, Mr. Chairman.

I want to thank you for holding this series of hearings that we are in process with today.

Mr. Hansen, I want to thank you for your time. I want to thank you for your interest and concern on this issue. And I want to thank you for being willing to take the time to come and be with us today.

In the past, child predators usually had to operate in person. They had to operate over the phone or through the mail in order to lure children. And now the Internet, with the availability and easy access to people, these child predators have many more tools at their disposal, and unfortunately, many times they are anonymous.

In past hearings, we have seen some of these tools that they use to solicit children, and today we are going to look at the methods that Internet companies can implement to protect children from being accosted by these despicable people. I know that some companies have recognized some of the means that the predators are using and are starting to implement more stringent steps to protect children from these predators.

But I want to remind the companies present at today's hearing that it is incumbent upon them to use all of the available technological tools to prevent child predators from gaining access to our children. That is your responsibility. Our constituents want action with results. They do not want half-hearted efforts on anyone's attempt. This is a problem that is out of control. It is a problem that we must arrest. It is a problem that we have to get our arms around, and collectively we have to solve this. We have to solve this.

These efforts are not a substitute for law enforcement, but more and more parents, including my constituents, are becoming increasingly concerned about online child predators, and they want to see children protected. They want to know that their children are safe when they are using the Internet. They want to know that you are their partner in protecting these children.

One issue that keeps recurring is how these companies are monitoring communications that would reveal either the transfer of child pornography or messages that would indicate that a user might be a child predator.

Mr. Chairman, I look forward to hearing from the companies today. I look forward to hearing from our first witness. And I thank everyone for their time.

[Additional statement submitted for the record follow:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY  
AND COMMERCE

Thank you, Chairman Whitfield, for convening this hearing.

Over the last six months, this subcommittee has been investigating the sexual exploitation of children over the Internet. Our previous hearings have left no doubt that the war against online child pornography and sexual exploitation is not merely a problem

for law enforcement to solve. Everyone must do his or her part to combat this epidemic of abuse if we are to succeed. And this includes the Internet Service Providers and social networking sites that will appear before this subcommittee today and tomorrow.

Law enforcement agents who testified during our previous hearings talked about what industry could do to help win the war against the online sexual exploitation of children. One of the problems the agents discussed was inadequate data retention. I think all the members of this subcommittee shared the agents' frustration when they described how some of their investigations were thwarted because Internet Service Providers had not retained the data that would allow them to make a link between an IP address used by an online predator and that predator's name and home address. In one instance, law enforcement was unable to find the man who was seen raping a two-year old child on an online video because the Internet Service Provider no longer had the IP address information that would have led the police to the predator.

In response to incidents like these, the Department of Justice has been meeting with Internet companies, including some of those appearing before us today, and has proposed a two-year data retention period. Just last week, Ranking Member Dingell and I received a letter from the National Association of Attorneys General urging Congress to study the issue of a national data retention standard. Therefore, I look forward to hearing your thoughts on these proposals. I understand data retention is a complex issue and that an extended retention requirement might pose cost increases for your companies. I am hopeful a solution can be reached that will satisfy the concerns of law enforcement and the concerns of the industry.

Another area where Internet companies assist law enforcement is by making reports to the National Center for Missing and Exploited Children. While the Internet Service Providers and social networking sites that are testifying today and tomorrow all report to the National Center, there are many other providers and sites that either ignore or are not aware of this reporting requirement. In addition to your views on data retention, I am interested in learning your thoughts on mandatory registration of ISPs to facilitate increased reporting to the National Center, as well as other ideas you may have to help law enforcement find these criminals who seek to abuse our children.

While reporting and data retention are two key tools that will help bring an end to online child pornography, industry's role in this fight cannot simply be limited to responding to law enforcement requests or reacting to the child pornography they discover on their networks. It is essential that industry get ahead of the problem — and the predators — by developing safeguards which will prevent these criminals from taking advantage of their networks and websites in order to send images of child abuse or to lure children. I understand that some of the companies that are appearing before us today announced just this morning that they are coming together to create the Center for Child Protection Technologies at the National Center for Missing and Exploited Children. This center will focus on developing technology solutions to detect and disrupt the transmission of child pornography. In addition, it will serve as a clearinghouse for known child pornography images that network operators can use to block child pornography. I commend the industry for launching this initiative. It is a valuable step towards winning the war against child pornography. We must make sure that every effort is brought to bear, as the price paid by the children who are victims of Internet child pornography and sexual exploitation is lifelong and devastating.

I look forward to hearing from the witnesses and yield back the balance of my time.

MR. WHITFIELD. Thank you, Mrs. Blackburn.

And I believe that concludes the opening statements, so Mr. Hansen, thank you for your patience.



We are delighted to have Chris Hansen here with us today from NBC News. And Mr. Hansen, as you probably are aware, in this Oversight and Investigations Subcommittee, we have a practice of taking all testimony under oath. And under the Rules of the House and the rules of the Committee, of course, you are entitled to legal counsel. I am assuming you don't need legal counsel today, so if you would please stand up, and I would like to swear you in.

[Witness sworn.]

MR. WHITFIELD. Thank you.

You are now under oath, Mr. Hansen, and you are recognized for a 5-minute opening statement.

### **STATEMENT OF CHRIS HANSEN, DATELINE NBC**

MR. HANSEN. Mr. Chairman and members of the subcommittee, thank you very much, and good morning.

I am Chris Hansen with Dateline NBC, and first off, again, I would like to thank the Subcommittee on Oversight and Investigations for inviting me to testify today on this critically important topic.

I would also like to thank you for understanding and accepting the limitations in what I can say as a member of a news organization.

A little more than 2 years ago, we set out to investigate computer predators: adults who go online into chat rooms and try to meet underage boys and girls.

Volunteers from the online watchdog group, Perverted Justice, posed as young teens home alone and open to the idea of an encounter. We rented a home in Long Island, New York, and outfitted it with hidden cameras. The decoys set up profiles in chat rooms that included pictures of boys and girls that were unmistakably underage. The decoys waited to be approached by men in the chat rooms. They didn't wait long. Within minutes sometimes, men were trying to start up inappropriate and often obscene conversations. There was graphic language, pornographic material, and a grooming process all geared at setting up a sexual liaison with a minor. The question was: would any of the men actually show up at our hidden camera house to keep their date with a young teen?

In the days before the shoot, I had wondered quietly to myself about the possibility that perhaps no one would show up. Maybe the anecdotal evidence we had seen on the computer predator problem was overstated. But as I was stuck in traffic on the Throgg's Neck Bridge headed to the house, I received a call from my producer, Lynn Keller, who was frantic. A man was due to show up in 45 minutes, and I had to be there. Fortunately, I made it there in about a half hour, leaving just enough time to prepare to confront the man before he walked in the door right on

schedule. For the next 2½ days, we witnessed a parade of potential predators. There were men from all walks of life. Even a New York City firefighter surfaced in our investigation.

Last summer, we continued our investigation, this time setting up a home in Fairfax County, Virginia, just miles from where we are now sitting. Again, Perverted Justice members worked as decoys, and the home was outfitted with hidden cameras. In 3 days, 18 men walked into the hidden camera house expecting to meet an underage boy or girl. There was a rabbi, an emergency room doctor, a special education teacher, and a man who walked in from the garage naked, carrying his clothes and a 12-pack of beer.

Earlier this year, we set up in a home in Southern California. This time, however, law enforcement set up a parallel investigation so the men could be arrested after I confronted them. In 3 days, 51 men came to the house to meet a boy or a girl and were arrested. Again, there was a wide range of characters: a teacher, a lawyer, an actor, even a Federal agent assigned to the Department of Homeland Security. And there was something we had not seen before: a number of previously convicted sex offenders. One of them was a 68-year-old man who had recently pleaded guilty to having sex with a 15-year-old boy. He was on probation as he walked into our home to meet someone who told him online he was 13. Another man who showed up had an even darker past. Our investigation revealed that 20 years before he walked into our house, he had molested three children in the same family in Oregon. Their mother had met the man through a mentoring program. And the trail didn't end there. It turns out he had yet another conviction in Palm Springs, California, after that.

The Southern California investigation drew men all of the way from Los Angeles to San Diego. We wondered if this was a big city crime or if we would find computer predators in small-town America as well.

Our next investigation took us to Darke County, Ohio, population 13,000. Would potential predators travel miles of country roads, past cornfields and cow pastures to visit a child home alone? The answer was yes.

Even though word of our investigation leaked out in the small town of Greenville, Ohio, where we had set up, 18 men came to our house after explicit online conversations with a decoy from the watchdog group Perverted Justice. All of them were arrested after we confronted them. It was here in Ohio that we saw something new: a growing number of men who showed up had actually seen some of our past investigations and came anyway.

A sixth-grade teacher who came to meet a 13-year-old girl admitted to me that not only had he seen our past broadcasts, but he had actually

discussed them with his fellow teachers. Another man who had showed up at our Ohio house late on a Sunday night was scheduled to go to jail in just 4 days for earlier soliciting a child online. Since then, he has pleaded guilty to molesting a young female relative in yet another case.

Our most recent investigation took us to Fort Myers, Florida, where in 3 days, 24 men showed up to meet a boy or a girl and subsequently were arrested. After five investigations in five different States, we thought we had seen it all, but no one was prepared for what we saw next in Fort Myers. Late on a sunny Sunday afternoon, our hidden cameras were rolling as a 40-year-old man parked his SUV in front of our home. He had set up a date for sex with a decoy posing as a 14-year-old boy. We watched as he got out and walked around the rear passenger door. We suspected he may be grabbing some beer or food, as we had seen some other visitors do. Instead, he takes his 5-year-old son out of the car seat and leads him by the hand up the driveway towards the back door of our house. There was an audible gasp inside the house. After he walked in, I told him who I was and what Dateline was doing. I didn't want to scare his son. Fort Myers police, who had set up their parallel investigation in the nearby home, saw the man had brought his child. A female officer scooped up the boy so he did not have to further witness his father's arrest. Police called the boy's mother, who was at work, and she picked him up at the police station.

In all, nearly 130 men have surfaced in our five investigations. Ninety-eight of them have been charged criminally. Seven have pleaded guilty. The rest are awaiting trial and have pleaded not guilty.

What did these men have in common? The majority of the men don't stand out in a crowd. Most look like the guy standing next to you in line at the dry cleaner's or at the grocery store. They don't have the word "predator" tattooed across their foreheads.

Virtually every day in this country, it seems a Federal or a local law enforcement agency does a sting operation targeting potential predators. Dateline has now done five in less than 2 years. You would think that would be a deterrent. Perhaps, for some. But for many other men, the desire to meet a teen for sex is too powerful. We have also seen men who think the odds of being caught are remote. In our last investigation, several visitors realized almost immediately what was going on. It was almost as if they were saying, "Oh, you are that guy. This is that show. And do you want me to sit over here?"

What drives these men? Based on our experience and what experts tell us, there is no one-size-fits-all characterization. Some are sexual opportunists who think they can take advantage of an inexperienced but curious teen. Some are evil. They are just wired wrong. Some are sick, perhaps victimized as a child. Many share an addiction to online chat

rooms and pornography sites and, eventually, a compulsion to meet a young teen for sex.

The anonymity and 24/7 access to the Internet can fuel this compulsion. In our experience, potential predators will sometimes talk to someone posing as a child for weeks before suggesting a meeting. There is a grooming process that often starts with casual banter: talk of hobbies, sports, or a troubled relationship with a parent. The potential predator will many times say he has shared in a child's experience. Often, the man will say early on that he is too old for the teen and he could get into serious trouble if they met. Then, however, the conversation will turn explicit. He will suggest different sex acts. A meeting is agreed to, and the next thing we see is him coming through the door.

Our reporting suggests it is not hard for a potential predator to find a teen to talk to. Regional chat rooms are often where our decoys are approached. The decoy never makes the first move. It is usually only a matter of minutes before he or she is contacted. The decoys pose as regular kids with regular issues. They are open to the idea of a visit and potentially a sexual encounter.

In our investigations, we have found that social networking sites are also popular trolling grounds for potential predators. MySpace, Xanga, and Facebook are places where teens often post personal pictures and information that they wrongly believe is only viewed by their friends.

The incredibly good news for parents and children is that experts tell us that there is no magic way for a potential predator to enter your home via the high-speed cable. Your child must provide information for a meeting to take place. That is why a dialogue between parent and child and teacher and student is so critical. It is really the same discussion our parents had with us years ago about strangers at the playground or accepting a ride from someone you don't know. You just have to apply it to the Internet.

I have brought with me today a DVD that has excerpts from some of our reporting. I would like you to see that, and afterwards, I would be happy to entertain questions.

[The prepared statement of Chris Hansen follows:]

PREPARED STATEMENT OF CHRIS HANSEN, NBC NEWS

Good Morning,

I'm Chris Hansen with Dateline NBC. First off, I would like to thank the Subcommittee on Oversight and Investigations for inviting me to testify today on this critically important topic. I would also like to thank you for understanding and accepting the limitations in what I can say as a member of a news organization.

A little more than 2 years ago we set out to investigate computer predators, adults who go on-line into chat rooms and try to meet underage boys and girls. Volunteers for

the on-line watchdog group Perverted Justice posed as young teens home alone and open to the idea of an encounter. We rented a home in Long Island, New York and outfitted it with hidden cameras. The decoys set up profiles in chat rooms that included pictures of boys and girls that were unmistakably under-age. The decoys waited to be approached by men in the chat rooms. They didn't wait long.

Within minutes sometimes, men were trying to start up inappropriate and often obscene conversations. There was graphic language, pornographic material and a grooming process all geared at setting up a sexual liaison with a minor. The question was: would any of the men actually show up at our hidden camera house to keep their date with a young teen.

In the days before the shoot, I had wondered quietly to myself about the possibility that perhaps no one would show up. Maybe the anecdotal evidence we'd seen on the computer predator problem was overstated. But, as I was stuck in traffic on the Throgs Neck Bridge, headed to the house, I received a call from my producer Lynn Keller. She was frantic. A man was due to show up in 45 minutes and I had to be there. Fortunately I made it there in about a half hour leaving just enough time to prepare to confront the man before he walked in the door right on schedule. For the next two and a half days we witnessed a parade of potential predators. There were men from all walks of life. Even a New York City firefighter surfaced in our investigation.

Last summer we continued our investigation, this time setting up in a home in Fairfax County Virginia, just miles from where we are now sitting. Again Perverted Justice members worked as decoys and the home was outfitted with hidden cameras. In 3 days 18 men walked into the hidden camera house expecting to meet an underage boy or girl. There was a rabbi, an emergency room doctor, a special education teacher and a man who walked in from the garage naked, carrying his clothes and a 12-pack of beer.

Earlier this year we set up in a home in southern California. This time, however, law enforcement set up a parallel investigation so the men could be arrested after I confronted them. In 3 days 51 men came to the house to meet a boy or girl and were arrested. Again, there was a wide range of characters: A teacher, a lawyer, an actor, even a federal agent assigned to the Department of Homeland Security. And there was something we had not seen before: a number of previously convicted sex offenders. One of them was a 68-year old man who had recently pleaded guilty to having sex with a 15-year old boy. He was on probation as he walked into our home to meet someone who told him on-line he was 13. Another man who showed up had an even darker past. Our investigation revealed that 20 years before he walked into our house, he had molested 3 children in the same family in Oregon. Their mother had met the man through a mentoring program. And the trail didn't end there. It turns out he had yet another conviction in Palm Springs, California after that.

The southern California investigation drew men all the way from Los Angeles to San Diego. We wondered if this was a big city crime or if we'd find computer predators in small town America as well. Our next investigation took us to Darke County, Ohio, population 13-thousand. Would potential predators travel miles of country roads, past corn fields and cow pastures to visit a child home alone? The answer was: yes. Even though word of our investigation leaked out in the small town of Greenville where we were set up, 18 men came to our house after explicit on-line conversations with a decoy from the watchdog group Perverted Justice. All of them were arrested after we confronted them. It was here in Ohio that we saw something new. A growing number of the men who showed up had actually seen some of our past investigations and came anyway. A 6<sup>th</sup> grade teacher who came to meet a 13-year old girl admitted to me that not only had he seen our past broadcasts, but he had actually discussed them with his fellow teachers. Another man who showed up at our Ohio house late on a Sunday night was scheduled to go to jail in just 4 days for earlier soliciting a child on-line. Since then he's pleaded guilty to molesting a young female relative in yet another case.

Our most recent investigation took us to Fort Myers, Florida where in 3 days 24 men showed up to meet a boy or a girl and subsequently were arrested. After 5 investigations in 5 different states we thought we had seen it all, but no one was prepared for what we saw in Fort Myers. Late on a sunny Sunday afternoon our hidden cameras were rolling as a 40 year old man parked his SUV in front of our home. He had set up a date for sex with a decoy posing as a 14-year old boy. We watched as he got out and walked around to the rear passenger door. We suspected he maybe grabbing some beer or food as we'd seen some other visitors do. Instead he takes his 5-year old son out of his car seat and leads him by the hand up the driveway towards the back door. There was an audible gasp inside the house. After he walked in I told him who I was and what Dateline was doing. I didn't want to scare his son. Fort Myers Police who had set up their parallel investigation in a nearby home saw that the man had brought his child. A female officer scooped up the boy so he would not have to further witness his father's arrest. Police called the boy's mother who was at work and she picked him up at the police station.

In all, 130 men have surfaced in our 5 investigations. 98 of them have been charged criminally. 7 have pleaded guilty. The rest are awaiting trial. What do these men have in common? The majority of the men don't stand out in a crowd. Most look like the guy next to you in line at the dry cleaners or the grocery store. They do not have "predator" tattooed on their foreheads.

Virtually every day in this country it seems a federal or local law enforcement agency does a sting operation targeting potential predators. Dateline has now done 5 investigations in less than 2 years. You'd think that would be a deterrent. Perhaps for some, but for many other men the desire to meet a teen for sex is too powerful. We've also seen men who think the odds of being caught are remote. In our last investigation, several visitors realized almost immediately what was going on. It was almost as if they were saying "oh, you're that guy, this is that show, this is where you want me to sit?"

What drives these men? Based on our experience and what experts tell us there is no one size fits all characterization. Some are sexual opportunists who think they can take advantage of an inexperienced but curious teen. Some are evil. They're just wired wrong. Some are sick, perhaps victimized as a child. Many share an addiction to on-line chat rooms and pornography sites and eventually a compulsion to meet a young teen for sex.

The anonymity and 24/7 access to the Internet can fuel this compulsion. In our experience potential predators will sometimes talk to someone posing as a child for weeks before suggesting a meeting. There is a grooming process that often starts with casual banter, talk of hobbies sports or a troubled relationship with a parent. The potential predator will many times say he's shared in the child's experience. Often the man will say early on that he is too old for the teen and he could get into serious trouble if they met. Then however, the conversation will turn explicit. He'll suggest different sex acts. A meeting is agreed to and the next thing we see is -him- coming through the door.

Our reporting suggests it is not hard for a potential predator to find a teen to talk to. Regional chat rooms are often where our decoys are approached. The decoy never makes the first move. It's usually only a matter of minutes before he or she is contacted. The decoys pose as regular kids with regular issues. They are open to the idea of a visit and potentially a sexual encounter. In our investigations we have found that social networking sites are also popular trolling grounds for potential predators. My Space, Xanga and Facebook are places where teens often post pictures and personal information that they wrongly believe is only viewed by their friends.

The incredibly good news for parents and children is that experts tell us that there is no magic way for a potential predator to enter your home via the high-speed cable. Your child must provide information for a meeting to take place. That is why a dialogue between parent and child and teacher and student is so critical. It's really the same discussion our parents had with us about strangers at the playground or accepting a ride from someone you don't know. You just have to apply it to the Internet.

I'll be happy to entertain questions.

MR. WHITFIELD. Thank you, Mr. Hansen. And we appreciate your bringing that videotape. And at this time, if you all would play it, we would like to look at it.

[Video.]

MR. WHITFIELD. Well, I don't know what to say, Mr. Hansen. That was quite a compelling video. And it is unbelievable that you were able to get all of that on TV. And I guess it has been shown throughout the country. And you are continuing to do this. But it certainly demonstrates the widespread problem that we have throughout our country.

And I guess the first question I would just like to ask you relates to this group Perverted Justice. Now could you explain a little bit about that group?

MR. HANSEN. Mr. Chairman, this is a group started by a fellow named Xavier Von Erck, who lives in Oregon. And they started as volunteers who essentially would go online posing as kids in chat rooms. If they caught an adult trying to set up a meeting, they would actually post information about this adult on their website. And you know, people could check it out and see who was taking part in this alleged behavior. We became aware of the group and thought maybe we could use their expertise in terms of their decoy work. And if we were able to use our hidden cameras and our technology to cover this crime, that we could watch them in action and, get a pretty compelling picture of what is going on in some of these Internet chat rooms. And that is kind of how it started.

MR. WHITFIELD. And so that group has been involved with you since that time?

MR. HANSEN. Each and every time. And I think you saw a woman named Del there, who is very talented when it comes to posing as a young girl or boy online. And she knows the teen speak of the Internet, as does Frag, the fellow you saw there. And they have contributors around the country who go online and they pose as kids in these chat rooms. And the information ultimately comes to the house where we are set up. Perverted Justice provides Dateline with the transcripts so we can go through them. And I read every word of them, so I am prepared when these guys come in. and in the last couple of investigations where law enforcement had a parallel investigation going, Perverted Justice would also provide transcripts of the chat log to the law enforcement, and they would be ready to take action on their part.

MR. WHITFIELD. Are there some specific chat rooms that seem to be used more than others, from your experience?

MR. HANSEN. Typically, these are regional chat rooms. There have been some that apparently have a reputation for, perhaps gay romance or regular romance, but they are not anything specifically set up for something that people might find different or out there or alternative, generally.

MR. WHITFIELD. All right. And all of these men that participated in these events, were they all prosecuted, from your knowledge, or do you know?

MR. HANSEN. In the very first investigation in Long Island, we didn't have law enforcement doing a parallel investigation, so to the best of my knowledge, the only prosecution that occurred there involved the firefighter who surfaced there. He pleaded guilty recently after facing Federal charges. In Washington, there was a handful of cases prosecuted, but to be honest with you, it is difficult for law enforcement and prosecutors to come in after the fact and, based on our broadcast and/or based upon Perverted Justice's chat logs to prosecute all of these men. In Fairfax County, Virginia, they did as best as they could. Once law enforcement started having a parallel investigation, then, obviously they are in on it from their standpoint from the beginning, and they are able to make their cases.

MR. WHITFIELD. Of course, you had one gentleman who brought his 5-year-old son. You had one gentleman who came in nude. And did you have other examples of people bringing their children with them to these encounters?

MR. HANSEN. No, nobody has, in the past, brought their children, but to see that video is stunning, but we work with 20 or so people inside this house, and these are guys who have been with me in India and investigations in Cambodia. They have been in tough places, dark places all around the world. I don't have to tell you that literally, I mean, these guys are people who have seen it and done it all. After this happened, I mean, these guys were in tears. That is how saddening this thing was.

MR. WHITFIELD. From the experiences that you all had with this program, most of the predators that showed up at the homes, did most of them have prior convictions or not?

MR. HANSEN. The vast majority did not have past contacts with law enforcement of any sort. In California, as you saw from the video clips, we saw the most previously-convicted sexual offenders of anywhere else. We had one case in Ohio, and there had been some other cases where guys that had actually been exposed by Perverted Justice. But the vast majority of the men who walked into our investigations had not had prior sexual convictions.

MR. WHITFIELD. And it is my understanding that maybe one person showed up twice?



MR. HANSEN. There was a case in Fairfax County, Virginia, the fellow who also showed up naked there, the next day, we were in the course of our investigation, and the Perverted Justice people are set up in an upstairs bedroom on their computer, and one of them calls me up in disbelief, and says, "Remember the guy who walked in naked last night? He is in a chat room trying to set up a meeting with a decoy posing as a 13-year-old boy."

MR. WHITFIELD. Unbelievable.

MR. HANSEN. So they set up a meeting at a nearby McDonald's restaurant, and we, of course, go out there. I mean, I didn't think he would show up.

MR. WHITFIELD. Right.

MR. HANSEN. But as we were sitting there with the crews, here he comes. He walks right into the McDonald's and walks right out. I am standing there, and he said, "Well, I am just getting something to eat." And I said, "Well, look, this is our second time down this road, and I have got the transcripts." And he finally said, "I am sorry," and, "I am seeing a counselor."

MR. WHITFIELD. So were you ever personally threatened in any of these encounters?

MR. HANSEN. Nothing serious. I think, as you saw, the rabbi became upset and agitated, but it wasn't--

MR. WHITFIELD. I guess they are so shocked they can't respond at all.

MR. HANSEN. Well, I think a couple things happen. One, obviously, we have got the element of surprise in these investigations. Two, and I have seen this more and more as we have continued, I think some of these people have wanted to get help for some time and are almost relieved that they are caught. And I think because I am generally curious to know what these guys are thinking, they sometimes want to get it off their chests even though they know it could be on national television.

MR. WHITFIELD. I think the thing that is really disturbing about all of this is that these are examples that we know about that you were involved in, and just think of the thousands that are out there going on every day that no one knows about. And so you have got these adults chatting with young people. And we know from testimony that we have had here in these hearings that they meet these pedophiles, and some people are selling sex on demand. There was a couple in Texas who were generating, I think, around \$2 million a month, sexually abusing their own 5-year-old child on demand.

Well, Mr. Hansen, thank you so much for being here, for focusing attention on this important matter.

And at this time, I will recognize the gentleman from Michigan.

MR. STUPAK. Thank you, Mr. Chairman.

Mr. Hansen, thanks for your work.

Any females come forth?

MR. HANSEN. That is an excellent question. Five investigations, five States, in only one investigation did we even have contact with a female potential predator, and in that case, she did not show up. Perverted Justice will tell us that they have only seen it a couple times in the 4 years that they have been doing these investigations. Experts in this field suggest that while we do see female predators, and you have seen the stories about the teacher and the student, there have been a number of them, female predators prefer to know who that person is. They don't like the anonymity. And the reality is, at least in our experience, it is a male-dominated crime.

MR. STUPAK. At any time, or in your conversations with Perverted Justice there, were you referred to other sites to view? From the time you have contact, maybe, until the time they would come to show up, did they--

MR. HANSEN. There were instances where the potential predator would suggest to the decoy, "If you want to learn about this sex act, I can either send you pictures or I can refer you to a website where this stuff exists." Yes.

MR. STUPAK. How often did that happen or occur? Just a guesstimation.

MR. HANSEN. Yes, I mean, I think it happened a half a dozen to a dozen times over the five investigations.

MR. STUPAK. Is it fair to say that most of these predators would have webcams?

MR. HANSEN. I don't know if I would say most, but yes, I would say at least half have webcams. And we see more and more. And that is why in the Ohio investigation we introduced the webcam to what we were doing. And when we had the actress who obviously looked much younger than she was, that was a very convincing thing. And once the potential predator saw that, it really engaged them.

MR. STUPAK. So your decoy would indicate they had a webcam?

MR. HANSEN. Exactly.

MR. STUPAK. Okay. You testified that MySpace, Xanga, and Facebook are popular trolling grounds for potential sexual predators. Can you explain how these websites may perpetuate child exploitation and why these social networking sites are so appealing to pedophiles?

MR. HANSEN. Well, I think that potential predators know that there will be a lot of children on some of these social networking websites. And some of them have implemented controls, and there are ways that a child can prevent most strangers from visiting their website. But like

anything else kids don't always pay attention to the rules or to the protections that are out there. And so you do see the potential, in some cases, for contacts to be made. And we have seen adults, for instance, and there have been criminal prosecutions along these lines, who pose as a 14-year-old girl and set up an identity to make friends with other 14-year-old girls and ultimately set up a meeting with somebody who is supposed to be a photographer, and you can imagine what happens next.

MR. STUPAK. Right.

MR. HANSEN. So there is the potential.

MR. STUPAK. Well, short of shutting these social websites down, can you think of any safeguards you would put on there?

MR. HANSEN. I think it really comes down to a parent having a realistic approach to this with their child, because kids will take the path of least resistance. You can't just say, "I am going to pull the Internet out of the house." In the first investigation, I had a group of kids, probably nine or ten, all 12 years old, and I said, "How many of you, a show of hands, have had an uncomfortable, sexually-charged contact on the Internet from a stranger?" Almost all of them raised their hands. I said, "How many told your parents?" None. They are looking at the ground. They are kicking their feet. And I said, "Well, why not?" They said, "We are afraid they are going to take the computer away." You have got to tell the kid, "Look, if this is going to happen, and it can happen, come to me. We will contact the law enforcement authorities. We will contact the Internet service provider." The Internet service providers don't want this stuff going on. But you have got to team up with your kid. You can't just bark orders and try and make the problem go away.

MR. STUPAK. I take it when your decoys were setting up their sites, they were easy to access, nothing real sophisticated to get into?

MR. HANSEN. Exactly. I mean, the chat rooms that they were in were, for the most part just basic regional chat rooms.

MR. STUPAK. We have estimates, and I think I used the figures in my opening statement that 1 in 5 will be contacted by a predator and 1 in 33 is convinced to contact the predator offline through a phone call, letter, or actually a visit. Is that consistent with what you saw?

MR. HANSEN. The one in five number comes from a study that is quoted by the National Center for Missing and Exploited Children.

MR. STUPAK. Right.

MR. HANSEN. We actually commissioned a study on our own that we had as part of the Ohio investigation that showed the number might be more like one in three, depending on how you define a sexually-explicit or sexually-suggestive contact. And the other hard thing there, obviously, is it sexually-suggestive contact by another teen or is it from

an adult? And that is not always easy to figure out. I mean the statistics, they are estimates, and you just have to keep that in mind that they are estimates, as best as we can get them.

MR. STUPAK. The other statistic I used in my opening, I indicated, and I think you brought it home with the man that showed up with his 5-year-old son, that about 35 to 40-percent of these people are known to abuse children, either their own or a close relative or something like that. A new study is going to be coming out here soon. They estimate that might be as high as 75 to 80 percent. Would you take issue with those numbers?

MR. HANSEN. I have no evidence that disputes that, but I should be clear--

MR. STUPAK. In your study, did you commission--

MR. HANSEN. We did not specifically address how many people who are taking this behavior on the Internet who also may or may not have inappropriate contact with their child. But in the case of the guy you saw in Fort Myers, Florida, just to be clear, based on his questioning by police, he was not going to, or he did not intend to involve his son in any sex act. He just happened to be babysitting that day, and the thought was that he could watch a video in another room while the father contacted the teen, or who he thought was a teen.

MR. STUPAK. Did any of these individuals show up with their own video camera to record whatever was going to happen?

MR. HANSEN. We have not seen anyone bring a video camera, but we have seen disposable cameras and regular cameras. And obviously there are phones that can take video, and we have seen some of that. Yes.

MR. STUPAK. You indicated in a question to the Chairman that you felt that some of these people were relieved to actually get caught. It seems like they are relieved to get caught, but where do you go with this? What do you do with this? How do you identify this? I guess that is what I am struggling with here.

MR. HANSEN. I think that what happens sometimes is we all want to just characterize these people as one sort of person, one solution, whether it is the criminal justice system or some sort of treatment, and it is just not the way it is. I mean, I have seen 21-year-old guys walk in there for a 14-year-old or 15-year-old girl, and they are probably lonely. I am not defending what these guys are doing, but--

MR. STUPAK. Right.

MR. HANSEN. --they are sad cases. I have seen some real heavy-duty cases of predators coming in there who if you read the chat logs, and you feel like you have to take a shower. So, I mean, are there guys who could go to counseling and be better if they are watched? Yes. Are

there guys who just can't be fixed by any other way than going to prison? There is that, too. But what has become clear is, and the experts we have interviewed on this topic say this as well, that there are not enough treatment opportunities. There is not enough counseling out there if a guy thinks he has got a problem. And I guarantee you, there are guys out there right now who are wondering about their Internet conversations and wondering if they are going over the line.

MR. STUPAK. This is more for the next panel, but just let me ask you this. We and our staffs, in preparation for these hearings, put in the words "pre-teen," "sex," and "video," and we did a search. We did Google, Yahoo!, and MSN. And it is quite interesting the way each of these service providers handled it. By that, I mean not only did you have the website, but then you had sponsored links on some of them, and then others were very good that had the sponsored links and you had to have a combination of words in order to access some of this. I mean, I would imagine the folks you dealt with deal with these sites all of the time. And let us get their curiosity up and get things rolling for them. Is there something, any suggestions you have for the ISPs coming up next?

MR. HANSEN. Well, I am not here to take a policy position for the ISPs or on any legislation or self-regulation, but I can tell you this, that in our experience, it is not uncommon for one of these guys who shows up at our house to have a pattern that starts with viewing pornography online, getting into graphic chats, and having an obsession or a compulsion that will ultimately lead him to try to meet a teen in person.

MR. STUPAK. Thank you. Thank you again for your work.

MR. HANSEN. My pleasure. Thank you.

MR. WHITFIELD. Mr. Walden.

MR. WALDEN. Thank you, Mr. Chairman.

Mr. Hansen, I am curious. How long does it take you to set up one of these sting operations, if you will let me use that term? What kind of timeline is involved? What kind of cost?

MR. HANSEN. We are on site for about 5 or 6 days, so it takes the tech people about 3 days to set up the house. I usually get in a day before we actually start shooting just to see the set-up. I mean, I have been told all about it from the planning process on.

MR. WALDEN. Sure.

MR. HANSEN. And we will start getting transcripts of chat logs in the days before, and I will start reading them and going through them with a highlighter, and then usually we do the actual part where the men arrive for 3 days.

MR. WALDEN. So in a week's time?

MR. HANSEN. In a week's time.

MR. WALDEN. That is from start to finish in a community?

MR. HANSEN. Correct.

MR. WALDEN. And what sort of costs are involved to do this?

MR. HANSEN. I am just not the budget guy on this.

MR. WALDEN. Somebody else's budget?

MR. HANSEN. That is somebody else's budget, and it is not a cheap thing to do, but it involves the hidden camera guys who are very specialized. It involves the regular camera crew.

MR. WALDEN. Let us take the camera piece out of it.

MR. HANSEN. Sure.

MR. WALDEN. Take the NBC, on air, we are going to film this, we are going to do interviews, we are going to do all of this out of it. To run one of these sting operations, absent that, would it be that hard for somebody to set up and run?

MR. HANSEN. Well, I think it takes a certain skill on the part of the person playing the decoy, and that takes some training, but obviously that is a learned skill. And I think obviously it can be done, because law enforcement agencies around the country are doing it. Polk County, Florida, just announced today or yesterday that they had nabbed 21 people, including some amusement park workers.

MR. WALDEN. In your work, what is the fewest number of people who have shown up to one of these houses? And what is the most?

MR. HANSEN. The fewest was the very first one where 17 men showed up in 2½ days, and the most was in Riverside County, California, where 51 men showed up in 3 days. And, I mean you could do it where you could have a guy showing up every 10 minutes, but from a practical standpoint and having time to talk to these guys and trying to get an understanding of what is going on in their heads you have to--

MR. WALDEN. You have to schedule them.

MR. HANSEN. --space them apart. Yes, and no matter what, obviously you have people bumping into each other in the driveway and then you would have long stretches where nobody shows up. And I don't mean to make light of it.

MR. WALDEN. No, and I don't either.

MR. HANSEN. It is a very serious topic.

MR. WALDEN. It is phenomenal.

MR. HANSEN. But clearly there are some moments like that that we see.

MR. WALDEN. And talk to me about the relationship with law enforcement. At some point in your program, you decided, "We are attracting these evildoers, if you will. We ought to be doing something more about it." Is law enforcement pretty interested in participating?

MR. HANSEN. Perverted Justice was contacted by the Riverside County Sheriff's Department, and they said, "Look, if you are willing to

work with us, we are willing to work with you. And if Dateline wants to do their parallel investigation that is fine, too.” And obviously, we don’t want to be an arm of law enforcement.

MR. WALDEN. Of course not.

MR. HANSEN. And law enforcement doesn’t want to be an arm of journalism.

MR. WALDEN. Right.

MR. HANSEN. So, we felt that with Perverted Justice kind of acting as the Chinese Wall in the middle, if you will, that we were able to preserve our integrity and they were able to preserve theirs, and we were able to operate.

MR. WALDEN. Have the Federal agencies shown an interest?

MR. HANSEN. Well, the Federal agencies do this a lot, and I visited FBI offices around the country and watched what they do, and they do it very well. Thus far, to my knowledge, no Federal agency has ever partnered with Perverted Justice at this point.

MR. WALDEN. Have they attempted that, from your knowledge?

MR. HANSEN. I don’t know that.

MR. WALDEN. During the course of the e-mail chats, does anybody observe that? Have you ever been, sort of, caught by an outside entity watching a chat, saying, “Something is not right here”?

MR. HANSEN. Oh, in other words, while we are acting as a decoy and a potential predator is talking to us and having an outside Federal agency doing their investigation? To my knowledge, it has not happened.

MR. WALDEN. Okay. And the ISPs, no involvement there?

MR. HANSEN. In terms of--

MR. WALDEN. They are not watching this? They are not--

MR. HANSEN. Well, I can’t speak for the policy of whatever monitoring goes on with the ISPs, but we have--

MR. WALDEN. That you know of.

MR. HANSEN. --never been contacted by an ISP saying, “What are you guys doing?”

MR. WALDEN. Yes, but do you know from your discussions with Perverted Justice? Have they been contacted when they are--

MR. HANSEN. Not to my knowledge.

MR. WALDEN. --being the decoy at all?

MR. HANSEN. I have never, honestly, asked them that question, but it would seem that that would be something that they would talk about and tell us about.

MR. WALDEN. Yes. It is just interesting how quickly you can attract 51 people to a site in less than a week’s time. And this stuff is going on

all of the time out there and you wonder who is kind of watching that, not that you want a lot of Big Brother on the Internet, but on this stuff--

MR. HANSEN. It also speaks to how vast the Internet is.

MR. WALDEN. Exactly.

MR. HANSEN. And I think one of the reasons we have continued in these investigations to see guys come in the door, aside from the compulsion or the obsession, is that the reality is what are the odds that it is Dateline. What are the odds that is a law enforcement agency?

MR. WALDEN. Well, you talk about how vast the Internet is, and yet when you go phishing, there are a lot of phish out there. They are on to your chat room immediately, it sounds like.

MR. HANSEN. Yes.

MR. WALDEN. What is the quickest response you have gotten?

MR. HANSEN. Oh, in minutes depending on the chat room and sometimes, as I said in my testimony, these guys will spend a long time, days, and you have got to remember that in some cases, Perverted Justice volunteers are actually out in the chat rooms before we are actually set up in the house.

MR. WALDEN. Right.

MR. HANSEN. So if they know where we are going to be operating, they may go out a week or two ahead of time and just start--

MR. WALDEN. Chatting.

MR. HANSEN. --putting them out there, chatting, and see what is going on. And so there might be a case where somebody shows up who has actually been in a conversation for a couple of weeks with somebody.

MR. WALDEN. But when you are talking about the vastness of the Internet, you are talking international. Here, you are talking about somebody who is going to drive or walk or take some mass transit to a site, so it is a very small circle, I would assume. What is the farthest away people have come?

MR. HANSEN. We have had people get on a bus and travel 4 hours to get from one side of Florida to the other.

MR. WALDEN. Wow.

MR. HANSEN. We had it happen in California, and we were in Riverside, and we had people come up from San Diego and up from LA and Hollywood. They are willing to travel.

MR. WALDEN. So it is not necessarily somebody in the neighborhood?

MR. HANSEN. Yes. I mean, in fact, probably the opposite is true. In Ohio, for instance, at least in the small town where we were, word got out that something was going on, and we had probably at least a dozen



local guys online who backed out. But we still had people traveling up from Cincinnati or from Dayton or from 2 or 3 hours away.

MR. WALDEN. So in other words, within their own network, they figured out something was going on?

MR. HANSEN. Something was up. Yes, they saw a lot of activity around the house. I mean, if Darke County's population is 13,000, it is--

MR. WALDEN. Somebody would drive by and see.

MR. HANSEN. Right. Greenville is probably a quarter to half of that, so somebody had figured it out.

MR. WALDEN. In your work as a journalist, have you ever been involved in anything more disgusting or shocking?

MR. HANSEN. And I am telling you, we just really didn't know what was going to happen the first time we were going to do it.

MR. WALDEN. Yes.

MR. HANSEN. But once they started coming in and it wasn't stopping, it really was an eye-opening experience as to how many people are out there willing to travel and take part in this activity.

MR. WALDEN. At a pretty high risk if caught.

MR. HANSEN. Depending on the State and depending on what they have done. We have seen the seven men who surfaced in these investigations who have pleaded guilty, one man in Riverside, California, had received 2½ years, and then we had another case in Ohio where a guy got 67 days time served and probation.

MR. WALDEN. That is it?

MR. HANSEN. I think that was the sentence. Now, there are other mitigating circumstances, and if you look at the chat, it may not have been as graphic as some of the others.

MR. WALDEN. All right.

MR. HANSEN. There is a whole lot that goes into it, so you can't necessarily compare them head on. But, depending on where you are and what the guy has actually done there is a wide range in the sentences. I mean, the previously-convicted sex offenders in California will obviously be looking at--

MR. WALDEN. Different issue.

MR. HANSEN. Yes.

MR. WALDEN. Any women involved?

MR. HANSEN. No. I mean, one time in the Virginia investigation we had somebody who identified themselves as a woman engaged in a chat but never showed up. And we just had not seen it in our investigations.

MR. WALDEN. And how many of the men then that have identified and participated, how many identified themselves as the age they are? Or do they try to mask it and say, "I am a 14-year-old, too," or, "I am 16."?

MR. HANSEN. We don't see so much people saying that they are 14 or 16. We see 60-year-old guys saying they are 40. We see 40-year-old guys saying they are 30 and 25-year-old guys saying they are 20 or 19, closer to the age of the potential target.

MR. WALDEN. All right. I sure appreciate the work you have done.

MR. HANSEN. Thank you.

MR. WALDEN. Thanks for being here today.

Thank you, Mr. Chairman.

MR. WHITFIELD. Ms. DeGette.

MS. DEGETTE. Thank you very much, Mr. Chairman.

Mr. Hansen, thank you for your testimony and also for your investigation.

As I mentioned in my opening statement, the NBC affiliate in Denver also did a similar investigation to what Dateline has been doing. Paula Woodward, who is a long-time investigative reporter there, did this. And it was the same result. They did it in conjunction with one of the local law enforcement authorities. I don't know if it was Perverted Justice that was the middle man, but they had, like, 40 or 50 guys show up at a house, and they were all arrested, too. And it was as you said. They were teachers and I don't know what all. But it is appalling. This is going on all around the country. So I bet you feel like maybe you should hang up your day job and just become an investigator someday.

MR. HANSEN. Well, you have seen it. There are stations in Milwaukee who have done it. You have seen it in Arizona, and I don't think that there is any geographic region that is immune from this.

MS. DEGETTE. Right. And it is just happening everywhere.

You deal a lot with law enforcement agencies in your investigations, and you talk to the State, local, and Federal investigators. Do they tell you about what kind of resources they have to try to find these child Internet predators?

MR. HANSEN. It is different in each jurisdiction. I mean, obviously the FBI has made this a priority issue. But like any other law enforcement agency, there is a lot going on at any given time. Darke County, Ohio, when we did that investigation, it was a big expenditure for them to do this over 3 days. But they felt it was important, and they did it.

MS. DEGETTE. Did they tell you they could use more resources?

MR. HANSEN. Well, I think, yes. Any law enforcement agency you talk to will tell you they could use more resources. But again, it is a matter of how often do you need to do it to get to the root of the problem? And I think that is different in every jurisdiction.

MS. DEGETTE. Well, as you said, though, apparently people weren't worried at all. One guy showed up 2 days in a row.

MR. HANSEN. Right.

MS. DEGETTE. So just doing one sting every so often, that is not necessary deterring these criminals. As you said, it has to be a whole program.

MR. HANSEN. Well, as we have seen, and as most recently as this spring when we were shooting in Florida guys were coming in. And before I could say "I am Chris Hansen, Dateline NBC," they were saying, "I know. I know. I know."

MS. DEGETTE. And yet they showed up anyway? It is almost like Candid Camera only with criminals that get arrested and go to jail. It is unbelievable.

MR. HANSEN. It is. I tell you, between reading every word of the transcripts and the interviews the 3 days, you are pretty much emotionally and, physically exhausted by the end of it. It feels like you had run a marathon.

MS. DEGETTE. Yes, I am sure. Do you know, are there any estimates as to how often online sexual predators are actually able to make contact with underage children and how often they actually then meet up with them in person?

MR. HANSEN. I think that would be a tough number to quantify just because there is so much going on out there that we don't know. I mean, again, we can go back to the figures that the National Center for Missing and Exploited Children uses or the figures that have come from our studies, but so many contacts potentially happen that you don't know about. It is a hard number to get. It is a hard estimate.

MS. DEGETTE. And it is a lot easier to go on to these chat rooms and talk to kids. I always say in the olden days, the sexual predators used to sort of have to lurk around the edges of parks or shopping malls. Now they can just go online, and it is a lot easier.

MR. HANSEN. Well, I also think that there are people perhaps who are taking part in this behavior, at least based on our experience, who would not necessarily have been hanging out at the movie theater or the park looking for a kid but have slipped into this behavior because of the obsession and compulsion that they have developed.

MS. DEGETTE. And you know, I was thinking about that when you were testifying, and I am wondering if you have an opinion as to what has suddenly caused so many more men to ease into that compulsion? Is it something in our society? Is it something about the anonymity of the Internet?

MR. HANSEN. Well, I think it is a little bit of both. I mean, the therapists we have interviewed who treat these men say it is a combination of the access, which is 24/7, the anonymity, which makes them bold, and the fact that, there are people out there to talk to who are

willing to engage in this conversation. It is no different than an addiction to gambling or anything else. It's just, for some people, a development.

MS. DEGETTE. And do you think those components kind of lead these men to think, "Well, it is all right if I do this?" I mean, of the men you have talked to, do they know, at some level, that it is wrong and, in fact, criminal?

MR. HANSEN. I think a lot of them do, and a lot of them have said to me when I have interviewed them that, "I was worried," including the teacher you saw in Ohio. "I was worried that I kept getting older but the people I was talking to were staying in the 12-, 13-, 14-year-old range." And he had talked about getting help, had thought about it, but didn't want to admit to himself there was a problem. And subsequent to that story, we found out that he had been chatting with an undercover officer in Carmel, Indiana, posing as a child and had exposed himself on the website and now faces a number of other charges there. So, our decoy wasn't the only one he allegedly was chatting with.

MS. DEGETTE. Right. Right. And I mean, that led me to something when you were talking to other members of the committee. It is true of these seven who have pled guilty, they got various sentences. They also lost their jobs, correct?

MR. HANSEN. That is correct, to my knowledge, in most of those cases.

MS. DEGETTE. I mean, these are people who, many of them, like you say, are teachers, rabbis. They are professionals. Just by being on your show, even if they are not criminally prosecuted, they are going to likely lose their jobs.

MR. HANSEN. It can have a negative consequence, yes.

MS. DEGETTE. Yes. And it seems to me that is one way--I mean, that is not a law Congress could pass, but that is one way society can really let people know this is not in any possible acceptable range of normal behavior. I mean, I think if professionals know that they are going to lose their jobs as well as be criminally prosecuted, they may think twice before they go down this road. What do you think?

MR. HANSEN. Well, I think it obviously ends up being, a lot of exposure. And, it is not just the charge that they are ultimately facing. It is the detail of what was in the chat log. And in some of these cases, when you go through and read it there is little doubt as to what the plan was.

MS. DEGETTE. What their intent is. One thing, aside from legislation, that we can do, States can beef up. We found out, in our first hearings, for example, that in my State, Colorado, one of the first examples that came out was some perpetrators in Florida who were raping a 4-year-old online. And it was in Colorado, my State. And they

tried to find the perpetrator through subpoenaing records through Internet service providers, and we found that the records had been destroyed, as they are routinely, so they never did find that perpetrator. And so that is one area that we think we can make legislation. And we are going to ask the second panel about that today.

The other thing we found out there is that, like in Colorado, it was a misdemeanor to be in possession of material like that. So I think my State legislators quickly fixed that in the end of the session. So there are different things that Congress can do. We can give more money to law enforcement agencies to prosecute and investigate these cases.

But one thing that I think you are saying, and I agree with you, it needs to be way beyond just passing laws. It needs to be sort of a societal, public service campaign involving the media and others.

MR. HANSEN. Well, I think you have seen, and you are probably familiar with the group, for instance, and there are many groups like this, I-SAFE, for instance, who we have interviewed for our stories. And they go to schools, and they have a campaign. And they have a website, and parents can go there. And it is a tutorial.

MS. DEGETTE. Yes, they came and testified. Yes.

MR. HANSEN. Yes. But they will tell you, this is step-by-step how you talk to your child about this.

MS. DEGETTE. Right.

MR. HANSEN. Your best defense, and I keep going back to this, and it is not a cop-out, I really believe it, is to start at home. And it starts with the parent and the child.

MS. DEGETTE. There is a group out of England who I met with, and they are actually part of an international group. They have got a public service announcement that they are showing in England that could be used everywhere. And Mr. Chairman, I think we should get them in and show this PSA. Maybe you have seen it, Mr. Hansen. It is targeted at these young kids and about how you get in a chat room and somebody starts taking you down this path, how you can get out of it.

MR. HANSEN. Right.

MS. DEGETTE. It is really an intense PSA. Oh, it is going to be shown tomorrow.

MR. WHITFIELD. Tomorrow, right.

MS. DEGETTE. And the response around here is always really snappy, and I appreciate it.

But it is an incredible public service announcement. I think your network and other networks should really look at doing this.

Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you.

Mr. Stearns.

MR. STEARNS. Thank you, Mr. Chairman.

Mr. Hansen, when your group set up these chat rooms, are there chat rooms that almost everybody in this country knows about? I mean, I have three children, and they were on the Internet, and I cautioned them about any chat room they were in. But I mean, are there, like, two or three chat rooms that everyone goes to? I mean, how did you find which chat room to go to or even which one to concentrate on?

MR. HANSEN. The vast majority of cases, it is just regular, old regional chat rooms, accessible through AOL or Yahoo!.

MR. STEARNS. So you went to AOL and then worked--

MR. HANSEN. And there were other ones, too. I mean, Perverted Justice sort of has a sense where there will be a lot of people where a lot of people from different walks of life will see this profile, which contains a picture of a boy or girl that is unmistakably underage, and they just sit there and wait. And you know, you will see a "Hey, what is up?" And "What is going on?" And "How old are you? You are way too young." And you know, it goes on from there.

MR. STEARNS. So it is easy for a 12- or 13-year-old person to find a chat room? Easy?

MR. HANSEN. Yes, I mean, some of these chat rooms, and the rules, change pretty quickly because of the ISPs are trying to, obviously, do their best to prevent this sort of activity from happening. But it is my understanding that if you want to get in a chat room, and even if there is a restriction on age, kids are crafty and they can get in there, if they want to.

MR. STEARNS. So if somehow we could set up, either through a software program or just like we rate motion pictures and we have ratings for videos, CDs, and we have some type of ratings now for video games, should chat rooms be set up with some kind of control from the Federal Trade Commission? Or in your opinion, should software be developed to set up categories where you--

MR. HANSEN. Well, I can tell you this. From a parent's point of view, software already exists that you can get for not a lot of money that you can set up at home that will actually sense if your child is giving out inappropriate or personal information. It will then e-mail you on your Blackberry, and you can pick it up and say, you know, "This is not good. I am going to call home." And say, "What the heck are you doing?"

MR. STEARNS. What is going on? That is excellent.

MR. HANSEN. Yes, it is. I mean, a lot of this stuff is out there. Parents just have to know about it. And of course, you have to realize that it is an issue and that it could happen in your home and it could happen to your kid even though they are a good kid. But, you need to have the discussion.

MR. STEARNS. So we should encourage manufacturers of computers to provide that software maybe?

MR. HANSEN. It is there.

MR. STEARNS. It could be just like you get your Microsoft Windows as part of the computer package. You may be able to get this, too. Sort of like a V-chip in the TV, you would have this software program be part of the package that you would buy, and the parents, or even anybody that bought the computer, could make the software available and could type in an e-mail so then that would be automatic, and then when the child goes on, he or she wouldn't know that they are being monitored by their parents.

MR. HANSEN. Yes. That technology exists as we speak.

MR. STEARNS. Okay. Okay. Well, I think all of us should realize and commend NBC for its trailblazing journalism here. I think what you are doing is highly commendable. I think you could take this same type of sting operation into many other areas, too. And I am sure it has crossed your mind.

MR. HANSEN. It has.

MR. STEARNS. The possibilities are endless. Out of the number that you saw in California and Florida, I thought it totaled about 190 people that came in. Just refresh my memory. How many?

MR. HANSEN. Fifty-one in California and twenty-four came in Fort Myers, Florida.

MR. STEARNS. Okay. So then that is 75.

MR. HANSEN. Correct.

MR. STEARNS. And you touched briefly on the profile of those 75. Some had past criminal activities. Verdicts of guilty and others were not. Was there any remarkable characteristic that you saw in terms of education of these people where they all seemed to be across? They either were rabbis, who obviously have a college education and beyond. They probably have a doctorate and a fireman who maybe had just a high school education. I mean, was there anything in the education area that came out at you?

MR. HANSEN. Not really. I mean, what most of these guys have in common is that they don't stick out of a crowd.

MR. STEARNS. Yes, they just--

MR. HANSEN. I mean, if you rode on a bus with them or a train they are regular guys, for the most part.

MR. STEARNS. Yes. Having raised three children and lots of them do go in chat rooms just to chat with their buddies or chat with other people, and I understand you have two children, too, what have you told your children or your wife or--

MR. HANSEN. Well, unfortunately for my kids, dad is a little more involved in it than some of the others, so I know most of the scams before they are even brought up at home. But in all seriousness, they watch the shows with me and--

MR. STEARNS. So they have watched--

MR. HANSEN. --we had the serious discussion and the continuing discussion with them. They happen not to be, at this particular moment, all that into IM-ing or chat rooms.

MR. STEARNS. Yes.

MR. HANSEN. They are more into the computer games. So it just hasn't been that big of an issue for us. But again, I just try to practice what I preach and say, "Look, you guys. This stuff is out there, and you have to be aware of it. And there are going to be people who try to trick you." And I think kids don't like to be tricked. And if you frame it that way you should get some response.

MR. STEARNS. Yes. Well, I think that is good, and I think it is also great that you brought to bear the understanding on this committee that there is software out there that monitors your children and what they are doing and can e-mail automatically to the parents. So in a way, the market can take care of this is what you are saying?

MR. HANSEN. Well, I certainly think that there are constructive software programs that we have seen and that we have showed in some of our stories that, as far as we know, work quite well.

MR. STEARNS. Yes. All right.

Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you.

Mr. Inslee.

MR. INSLEE. Thank you.

One of the more chilling aspects of this story and other discussions that we have had in the previous hearings is about the grooming that goes on by these predators that try to appear sort of innocent as they begin this relationship with their targets. Is there anything that you can advise parents about how to advise kids about that, either to spot it, what the warning signs are?

MR. HANSEN. Well, I think if you see, for instance, a package arrive for your child and in it is a webcam and they are dodging as to where it has come from, if phone calls start to arrive from strangers, if suddenly they have got a cell phone and they are not quite clear as to how they were able to get that cell phone, I mean those, the experts tell us, are all signals that somebody is trying to develop a way to communicate with your kid. And you saw with the Justin Berry case and Kurt Eichenwald's story in the New York Times how, you know, that webcam, for him was a gateway into this activity. So I am not saying there is anything



inherently even with webcams, clearly, but if this stuff starts showing up at your house and you don't know who is sending it, that is a signal. And we have seen it in our reporting that those are the kinds of things that a potential predator will offer.

MR. INSLEE. I wanted to ask you about what sort of observations you have for law enforcement. You have become an expert in sting operations, in a sense. Do you have any sense of what is possible for law enforcement? I mean, should we have, you know, 20 sting operations like yours up and running in this country at all times to have a more effective deterrent? Is that possible from a cost standpoint? Is it effective? Is it an effective deterrence? It is surprising to me that you have these shows on and these people still keep showing up, not only as viewers but participants. Do you have any thoughts about, for law enforcement, what they can do or should do?

MR. HANSEN. Well, I think law enforcement across the country is doing it, sting operations like this virtually on a daily basis. As I mentioned before, the FBI, on average, arrests, they call them "travelers," a traveler every day. We just saw the results of the investigation that the Polk County Sheriff's Office did. So there is a lot of this going on. And if you were to Google the subject, you would see in towns across America where it is happening. I don't know the extent to which it is a deterrent. Obviously, for some people, it will be. For others, as we have seen in our stories, you know, the compulsion or the obsession is stronger. We had a guy in California, for instance, who drove by the house and saw a previous arrest, called the Perverted Justice decoy and said, "Hey, there are cops in front of the house. What is going on?" She said, "No, it is just a drug bust going on next door. It is all done. Come on over." He comes in. It turns out Perverted Justice had caught him once before, and he had seen a previous story on Dateline. But this guy walked in the house anyway. Now whether that speaks to his lack of intelligence or the addiction or compulsion, it was probably a little bit of both, but, these guys, once they get it in their mind they want to do it, they want to show up.

MR. INSLEE. Right. Did you have any sense about sites that were particularly effective? Social sites that were either effective or ineffective in providing tools to protect kids? Did you have any sense of different approaches taken by sites that may work and may not work?

MR. HANSEN. Again, I think the best approach is the approach at home from a parent to a child. And if you are going to go on a social networking site, be smart about it. Don't let just anybody in. what we have seen in some of these cases is that, for instance, the decoy will have a profile set up in the chat room, but then after the discussion goes on, the potential predator will say, "Well, do you have a spot on one of these

social networking sites?" And the decoy will say, "Yes, and I will let you on," or, "I will accept you." And then it goes from there.

MR. INSLEE. Got you. Thank you very much for your work.

MR. HANSEN. Thank you.

MR. WHITFIELD. Thank you.

Mr. Bass.

MR. BASS. Thank you, Mr. Chairman.

And I just have one question of you, Mr. Hansen.

In the course of your investigation, did you uncover a lot of individuals who communicated who were under the age of 18?

MR. HANSEN. Most of the men who surfaced in our investigations from what I can recall, I don't think there was anybody under the age of 18.

MR. BASS. So it is your conclusion or your observation, rather, that this communication is not occurring, then, between people under the age of 18 who are looking for other people under the age of 18 to have a relationship with?

MR. HANSEN. I understand. I don't think I could draw that conclusion, because our story focused on adults who were seeking to meet children.

MR. BASS. Sure.

MR. HANSEN. We really didn't--

MR. BASS. Perverted Justice, they were your screen, is that right?

MR. HANSEN. Our decoys, correct.

MR. BASS. Your decoys. Are they testifying, Mr. Chairman, or not?

MR. WHITFIELD. No, they are not.

MR. BASS. Okay. I am just curious to know when they did the screen, what percent of the screen turned out to be people who were under the age of 18 versus over the age of 18. and there is no follow-up to that, because if this is a problem that is associated mostly, if not totally, with people who are over the age of 18 and that there really isn't much interest in this kind of communication for pre-18 to pre-18, it is an interesting observation. Are you suggesting that this might be the case or not?

MR. HANSEN. Well, I just don't think we know that. I mean, obviously there have been highly-publicized stories where kids have hooked up online, whether it is 18 and 16 or 19 and 16, as we saw the allegations most recently in Texas, but in our investigations the way they are set up, the decoy posing as a child is in a profile in a chat room and waits to be contacted. So I can only tell you that in our cases we haven't seen, to my knowledge, a lot of contacts from 15-, 14-, and 13-year-olds. The contacts are coming from adults, in our investigations.

MR. BASS. All right.

Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you, Mr. Bass.

And Ms. Baldwin.

MS. BALDWIN. Thank you. I will be brief.

Thank you very much for your testimony. And watching the images earlier, it shows such a great example of how investigative journalism is serving such an important educational role and prompting, I hope, communication between parents and their children.

What frightens me, of course, watching those images, is the fact that everyone says this is just the tip of the iceberg. And it is terrifying to think about how many children are being exploited and there is not a camera crew when the person walks into the house.

We have had a few questions about the limitations on law enforcement and the resources that are being dedicated to this. I am wondering whether, in the context of your show or perhaps through public service announcements, as we have talked about, if there is advice offered for parents or kids of what to do when there is an inappropriate Internet contact, who to call, who to alert, who to ask for an investigation. It seems to me that that is sort of the missing ingredient in this conversation of okay, you are promoting the dialogue between children and parents to prevent this, but what if you haven't prevented it? What does a parent do next?

MR. HANSEN. Well, I think in this time, when this subject is getting so much publicity, that I would just be shocked if a police department wasn't interested in investigating a case like this. I mean, every day another police department sets up, you know, a division dealing with this sort of thing, from Los Angeles to New York and everywhere in between. So you report it to the police, you report it to the Internet service provider. And I would say, in most cases, something will happen.

MS. BALDWIN. Thank you.

Mr. Chairman, I yield back.

MR. WHITFIELD. Thank you.

Mrs. Blackburn.

MRS. BLACKBURN. Thank you, Mr. Chairman.

And I have got just a couple of questions. I am going to continue on Ms. Baldwin's line of talk, because we know that many of the service providers are beginning to partner with PTAs and are looking at a multimedia, if you will, way of communicating with parents so that there are things going home with children in their backpacks and their money packs that they take home, that they are looking at partnerships, printing material, TV ads, as well as online information.

And all of that is good, but I want to look at what we should also consider doing as a legislative body. And I have been so intrigued with your partnership with Perverted Justice and the work that they have done. And what I would like to hear from you, and you can submit this in writing or your staff, but I would like to know what suggestions those guys that have actually worked the keyboard and assisted you with this investigation, Perverted Justice members and also your staff, as they have worked through this process. I am certain from time to time they have had a little nugget where they said, "They probably could do this," or, "I bet you they could write this into the program that would boot something out." And I would love to know if you were willing to share those nuggets with us what their thoughts have been, what their suggestions would be for us, and what they would have wanted us to know as we have worked on this hearing.

MR. HANSEN. Well, I can tell you this, that the people we have met from Perverted Justice are very savvy computer people, and I am sure that if you requested it, or if we requested it, I don't want to speak for them, but I am confident that they would be more than willing to assist you and give you any thoughts they have on it.

MRS. BLACKBURN. And your staff, also.

MR. HANSEN. Absolutely.

MRS. BLACKBURN. I know that it takes a dedicated and hardworking staff to be able to work through a 2-year project, a 2-year investigation, and that there has to be an incredible amount of knowledge gleaned that would serve us well.

MR. HANSEN. Absolutely.

MRS. BLACKBURN. Thank you.

I yield back, Mr. Chairman.

MR. WHITFIELD. Thank you, Mrs. Blackburn.

And Mr. Hansen, we want to thank you once again for being with us this morning and afternoon and for bringing us a new perspective on this whole issue. And we look forward to continue working with you and following your investigative reports.

So with that, you are dismissed. And best wishes.

MR. HANSEN. Thank you, Mr. Chairman. I appreciate it.

Thank you all.

MR. WHITFIELD. At this time, I would like to call the second panel.

We have on the second panel Mr. John Ryan, who is the Chief Counsel, Compliance and Investigation, America Online. We have Mr. David Baker, Vice President, Law and Public Policy for EarthLink, Inc. We have Ms. Elizabeth Banker, who is the Associate General Counsel for Yahoo!, Inc. We have Mr. Tom Dailey, who is the General Counsel for Verizon Communications. We have Mr. Philip Reiting, who is the

Senior Security Strategist for Microsoft. We have Mr. Gerard Lewis, Jr., Vice President, Deputy General Counsel, and Chief Privacy Officer for Comcast Cable. And we have Ms. Nicole Wong, who is the Associate General Counsel and Chief Privacy Officer for Google, Incorporated.

I want to welcome all of you. We thank you very much for your willingness to testify on what we consider to be a particularly important subject matter. And as you saw with the first panel, Mr. Hansen, we do take testimony under oath, and I would ask you, do any of you object to testifying under oath? And under the Rules of the House and the rules of the Committee, you are certainly entitled to legal counsel, but I am assuming you all do not need legal counsel. So if you would not mind standing and raising your right hand.

[Witnesses sworn.]

MR. WHITFIELD. Thank you very much. You are now under oath.

And Mr. Ryan, we will recognize you for a 5 minute opening statement. Thank you.

**STATEMENTS OF JOHN RYAN, ESQ., CHIEF COUNSEL, COMPLIANCE AND INVESTIGATION, AMERICA ONLINE, INC.; DAVID BAKER, VICE PRESIDENT, LAW AND PUBLIC POLICY, EARTHLINK, INC.; ELIZABETH BANKER, ASSOCIATE GENERAL COUNSEL, YAHOO! INC.; TOM DAILEY, GENERAL COUNSEL, VERIZON COMMUNICATIONS; GERARD J. LEWIS, JR., VICE PRESIDENT, DEPUTY GENERAL COUNSEL & CHIEF PRIVACY OFFICER, COMCAST CABLE COMMUNICATIONS; PHILIP R. REITINGER, SENIOR SECURITY STRATEGIST, MICROSOFT CORPORATION; AND NICOLE WONG, ASSOCIATE GENERAL COUNSEL & CHIEF PRIVACY OFFICER, GOOGLE, INC.**

MR. RYAN. Thank you, Mr. Chairman and members of the committee.

My name is John Ryan, and I serve as Chief Counsel for America Online. In that capacity, I oversee our efforts to assist law enforcement and to keep criminal activity off our networks. Additionally, I am privileged to serve as a member of the Board of Directors at the National Center for Missing and Exploited Children and serve as chairman of their Law Enforcement Committee.

Prior to joining AOL, I was a prosecutor in New York where I investigated and prosecuted numerous high-tech crimes, including crimes against children. I am a founding members of the Electronic Crimes Task Force in New York, which has been used as the model for the

cooperation between law enforcement and industry in the prosecution of electronic crimes.

AOL applauds the efforts of this committee in addressing the twin scourges of child pornography and child predation on the Internet. AOL has been fighting the spread of these plagues, both on our network and on the Internet for over a decade. The single guiding principle for America Online has been, and continues to be, the protection of children online.

AOL has pioneered the use of innovative technologies to protect our children. It has implemented industry-leading practices and policies that have been both adopted by others in the industry and included into State and Federal legislation.

AOL has staked its brand and reputation on providing a safe haven for children on our service. For AOL, these efforts make good business sense, but more important, are the right thing to do.

As this committee is well aware, these crimes represent a particular challenge, because they are facilitated by computers and the Internet. The challenges created by technology should be addressed by technology as well. Three years ago, AOL implemented extremely effective technologies to identify and remove abhorrent images of child pornography and to eliminate their transmission on our network. AOL developed a process that creates unique digital signatures from apparent pornographic images of children and uses those signatures to eliminate further dissemination of those images. AOL has assembled a library of these images and their signatures, and if AOL discovers that someone is trying to send a file over our network with a signature from that library, we prohibit the transmission of that file and refer that image to the National Center for Missing and Exploited Children to be investigated and prosecuted. Once the signature of the image is identified and referred to NCMEC, AOL deletes all record of the image and only retains the signature for future identification of bad images.

At AOL, we believe that proven technologies such as these make it harder for criminals to use the Internet to commit these crimes against children. AOL is committed to developing and deploying more promising technology to take back the Internet from those who would exploit or harm our children.

Although AOL has taken a leadership role in the development of best practices and solutions, we recognize that as technology evolves and criminals become more sophisticated, much more needs to be done. It is also clear that many members of this committee are very concerned about protecting children and want more to be done.

In response, AOL has developed a proposal to address these concerns in the most effective manner. Specifically, AOL commits to:

one, voluntarily preserve all relevant records relating to a report by an ISP to the National Center; two, support a legislative branch of authority to NCMEC to send preservation letters to ISPs upon review and determination that the referred images are child pornography; three, build and expand upon AOL's digital signature technologies and to share it with other industry colleagues to expand its reach; four, investigate new and innovative technologies to make the Internet a dangerous place for predators but not legitimate users; and five, most importantly, work with law enforcement to identify tools that will assist them in their critical work.

As a demonstration of our commitment, AOL has joined with a team of companies, including EarthLink, Microsoft, and Yahoo!, who are with me here today, to develop effective technologies to investigate and prevent child pornography online and also to provide financial and personnel resources to the National Center to further these efforts. These measures will ensure that law enforcement has all of the necessary data resources and tools so that they can pursue a successful investigation.

The primary objective at AOL is to ensure that children never become victims of online predators or become exposed to inappropriate content. Over the past decade, AOL has developed state-of-the-art parental controls that give parents the ability to block their children from receiving harmful content. AOL parental controls are broken down into three age categories: kids only, for ages 12 and under; young teen, for 13- to 15-year-olds; and mature teen, 16- and 17-year-olds. The controls provided include the ability to block e-mails, instant messages, or chat with unknown persons or specific individuals. Parental controls provide chat rooms if parents enable such access that are fully monitored by internal AOL enforcement teams. In light of the video that Mr. Hansen just provided, I think, and the questions were raised of this panel, of the concerns, AOL has addressed those concerns by providing a kids-online gated community where access to those chat rooms are controlled by the parent and are fully monitored by AOL staff. Anyone under the age of 16, when parental controls are activated, are not able to get outside of that gated community and access the Internet at large.

AOL parental controls, in combination with its Web Guardian Program, also have other practical features to empower parents to manage their child's use of the service, including: online timers to limit the amount of time a child stays on AOL; a report to parents, over one million weekly, a report card, so to speak, on the child's activity online, such as every website their child visits, which sites they tried to visit but were blocked from accessing, and how many e-mails and instant messages they sent; state-of-the-art, real-time web filters that allow older teens to access a broader range of content while still blocking offensive

material and controls to prevent bypassing of these protections. Only the master account screen name, which is controlled by the parent or guardian, is empowered to implement these controls and a sub account, which could be accessible by a minor, is disabled from amending or deleting those controls. We recognize that children are very Internet-savvy. Finally, our programs offer positive alternatives with a complete range of age-appropriate programming for these accounts, appropriate while blocking offensive sites.

Even with these extensive efforts, AOL knows that there are individuals who will send inappropriate content over our network or attempt to use AOL to lure children offline. To combat these attempts, AOL has long included a visible and convenient "Notify AOL," a report button, which is in every service that we offer to our members. And this is directed to a trained staff dedicated 24/7 to receive and review these reports and take appropriate action, including the referral of potential criminal activity to law enforcement.

In addition, beginning in the 1990s, AOL established contacts with State and Federal law enforcement agencies throughout the United States to whom AOL could refer the child pornography images and other identifying information for follow-up investigations. In 1999, this practice was codified into Federal law, and this was subsequently amended to designate the National Center as the sole recipient for referrals of child pornography.

MR. WHITFIELD. Summarize, please.

MR. RYAN. Let me summarize.

We are aware, despite these proposals and ongoing commitment that this committee must come up with new strategies, which one of them has been referred to as data retention. Our discussion is concerned about some of the potential drawbacks of data retention, namely the security of the databases that will be created. And more importantly, we believe at AOL the diversion of critical resources to maintaining and managing that repository of data from the real-time active investigations, which we currently support. So we welcome the ongoing dialogue, and we will work with this committee and others to come up with real solutions.

Thank you.

[The prepared statement of John Ryan follows:]



PREPARED STATEMENT OF JOHN RYAN, ESQ., CHIEF COUNSEL, COMPLIANCE AND  
INVESTIGATION, AMERICA ONLINE, INC.

June 27, 2006

Mr. Chairman and members of the Committee, my name is John D. Ryan, Chief Counsel at AOL, where I oversee our efforts to assist law enforcement and keep criminal activity off our networks. Prior to joining AOL, I was a prosecutor in New York where I investigated and prosecuted numerous high tech crimes, including crimes against children. I am a founding member of the Electronic Crimes Task Force in New York, which has been used as the model for the cooperation between law enforcement and industry in the prosecution of electronic crimes.

AOL applauds the efforts of this Committee in addressing the twin scourges of child pornography and child predation on the Internet. AOL has been fighting the spread of these plagues both on our network and on the Internet for over a decade. The single guiding principal for AOL has been and continues to be the protection of children online. AOL has pioneered the use of innovative technologies to protect children online. It has implemented industry leading practices and policies that have been both adopted by others in the industry and included into state and federal legislation. AOL has staked its brand and reputation on providing a safe haven for children online. For AOL, these efforts make good business sense, but more important, are the right thing to do.

As this committee is well aware, these crimes represent a particular challenge because they are facilitated by computers and the Internet. The challenges created by technology should be addressed by technology as well. Three years ago, AOL implemented extremely effective technologies to identify and remove abhorrent images of child pornography and to eliminate their transmission on its networks. AOL developed a process that creates unique digital signatures from apparent pornographic images of children and uses those signatures to eliminate further dissemination of those images. AOL has assembled a library of those image signatures and, if AOL discovers that someone is trying to send a file over our network with a signature from that library, AOL prohibits the transmission of that file and refers that image to the National Center for Missing and Exploited Children (NCMEC) to be investigated and prosecuted. Once

the signature of the image is identified and referred to NCMEC, AOL deletes all record of the image and only retains the signature for future identification of bad images.

At AOL we believe that proven technologies such as these make it harder for criminals to use the Internet to commit these crimes against children. AOL is committed to developing and deploying more promising technologies to take back the Internet from those who would exploit or harm our children. AOL is also committed to working with industry develop and implement these technologies widely. As I will discuss in more detail later, AOL has assembled a coalition to focus on these efforts.

The primary objective at AOL is to ensure that children never become victims of online predators or become exposed to inappropriate content. Over the past decade, AOL has developed state-of-the-art parental controls that give parents the ability to block their children from receiving harmful content. AOL Parental Controls are broken down into three age categories: Kids Only for ages 12 and under; Young Teen (13 – 15); and Mature Teen (16 and 17). The controls provided include the ability to block email, instant messages, or chat with unknown persons or specific individuals. Parental Controls also provide chat rooms, if parents enable such access, that are fully monitored by internal AOL enforcement teams.

AOL Parental Controls also have practical features to empower parents to manage their child's use of the service. There is a simple online timer to limit the amount of time a child stays on AOL. For AOL broadband users, AOL also provides Internet access controls for the PC, which will prevent a child from bypassing Parental Controls.

AOL Parental Controls do not merely restrict a child's access to potentially harmful encounters on the Internet, they provide positive alternatives with a complete range of age appropriate programming for parentally controlled accounts. For Mature Teens, AOL has state-of-the-art web filters that allow older teens to access a much broader range of content while still blocking offensive content. AOL filters are able to rate the content of pages in real time and only deliver those pages that are appropriate, while blocking offensive sites. This gives teens the flexibility to use the web while providing the maximum protection

AOL also has a feature called Web Guardian that allows parents to keep track of where their children visit and their activities online. Parents who subscribe to the service receive a list for every session on AOL detailing every website their children visit, which sites they tried to visit but were blocked from accessing, and how many emails and IMs they sent. AOL provides over 1 million AOL Guardian reports to parents every week.

AOL knows that there are individuals who send inappropriate content over our network or attempt to use AOL to lure children. From the beginning, AOL has included a visible and convenient "Notify AOL" button for members to report unacceptable behavior they encounter on our network to teams of trained professionals in the AOL Members Services department. Among the items reported are images of child pornography. Since child pornography is contraband and illegal to possess or distribute,

AOL realized over a decade ago that this material belonged in the hands of law enforcement so that it could be prosecuted. Beginning in the mid 1990's, AOL established contacts with state and federal law enforcement agencies throughout the United States to whom AOL could refer the child pornography images and other identifying information for follow up investigations and prosecutions. In 1999, this practice was codified into Federal law in 42 USC § 13032, which was subsequently amended to designate the NCMEC as the sole recipient for referrals of child pornography.

Congress, through 42 USC § 13032, directed ISPs to refer the facts and circumstances concerning all images of apparent child pornography of which they became aware to NCMEC. AOL consulted with NCMEC to determine what information was needed and what format would best facilitate the transmission of the information. As a result of that partnership, AOL became the first ISP to electronically transmit the referrals of child pornography. AOL went well beyond the strict mandates of the law and provided the offending image, the screen name associated with the image, and the zip code on the account. Through this process AOL ensured that law enforcement would have the offending image and all of the information necessary to send the case to the appropriate law enforcement agency for follow-up. The simple act of including a zip code eliminated days and weeks of lost time spent identifying and forwarding the report to the right agency for investigation.

The reports that AOL received from its members and the information observed in monitored chat rooms also uncovered attempts by pedophiles to solicit children. Rather than ignore this troubling information, AOL once again partnered with NCMEC to establish a child solicitation referral process, similar to the referral of child pornography. NCMEC shared its expertise in identifying predatory behaviors and trained AOL personnel to spot this behavior in communications they review. If a communication that is reported or observed in monitored chat rooms indicates the real possibility a child is being targeted online, AOL sends a report of the communication to NCMEC. In circumstances where the threat indicates the possibility that a meeting could take place within 72 hours, AOL sends the report directly to law enforcement in the location where the child resides. This approach is not mandated by any statute, but it is the right thing to do. AOL has been informed that in the 2 ½ years of its existence, this program has lead to 153 arrests. That is 153 or more children who were protected from abuse at the hands of a predator.

AOL's early experience showed that pedophiles do not take nights, weekends, or holidays off. As a result, in 1996, AOL initiated a 24/7 law enforcement hotline. However, there was no law providing ISPs immunity for giving information to law enforcement without process in the event of life threatening injury. AOL instituted a policy by which law enforcement officers could obtain the information if they identified the information as necessary due to a life threatening situation. In the years that followed, AOL provided law enforcement with information to help hundreds of real and potential victims of violence, including children. In 2001, the policies of AOL were reflected in Federal law in 18 USC § 2702, which allows ISPs to provide transactional

information and content to law enforcement on a showing of risk of death or serious bodily injury to a victim.

When Congress passed the Nationwide AMBER Alert law, AOL reached out to NCMEC and became the first ISP to initiate an Amber Alert program by which AOL members can receive email alerts targeted to their area. To date, over 365,000 AOL members have signed up to receive Amber Alerts. This program is unique and innovative and again demonstrates AOL's unflagging commitment to use the power of its network to provide protection to its users and others.

AOL knows only too well that crimes on the Internet pose particular challenges for law enforcement. Police and prosecutors frequently need special assistance in dealing with the unique challenges presented by investigating computer and Internet crimes. AOL has a team of highly trained and dedicated professionals, including former prosecutors, to assist law enforcement on tens of thousands of cases per year. They provide information in response to law enforcement requests, answers officers' questions on what types of information would help their cases, and provide guidance on obtaining the right information.

AOL has demonstrated an ongoing commitment to deliver cybercrime, digital evidence, and computer forensic science education to police and prosecutors through out the United States. AOL personnel teach at the FBI Academy in Quantico, Virginia, in the FBI Cyber Investigations Techniques & Resources programs. AOL personnel also teach Immigration and Customs Enforcement (ICE), IRS, ATF, and US Secret Service agents at a similar law enforcement education course at the Federal Law Enforcement Training Center in Glynnco, Georgia. Since 1999, AOL instructors have taught law enforcement education courses to the nation's criminal prosecutors at the US Department of Justice's National Advocacy Center (NAC) in Columbia, South Carolina eight to ten times per year. AOL has participated in the NAC's Justice Television Network (JTN), which has produced eight separate episodes dealing directly with AOL-related investigations within their "E-Vestigations" series.

AOL sits on faculties, panels, technical and scientific working groups, and committees within the National White Collar Crime Center, the National Center for Missing and Exploited Children (NCMEC), the National Center for the Prosecution of Child Abuse, the National Center for Forensic Science, the American Prosecutor Research Institute and the National Association of Attorneys General. Each of these organizations conducts law enforcement training in which AOL provides technologists and resources throughout the year. Starting in 2000, AOL committed to provide technologists to NCMEC's law enforcement training programs for investigators and prosecutors. Since then, thousands of agents, investigators, and prosecutors have heard the AOL law enforcement educational sections within the programs "Protecting Children Online for Investigators" (PCO) and "Protecting Children Online for Prosecutors" (PRO). Given the global impact of the Internet, AOL has also trained international law enforcement officials at Interpol in Lyon, France.

Since 1995, AOL has offered to the government, at no charge, litigation support, as well as fact and expert witness testimony on criminal cases involving records obtained from AOL. Each day, AOL receives dozens of inquiries and requests from law enforcement officials who ask for assistance with the many aspects of computer/Internet related criminal cases. Each request for litigation support or testimony from a prosecutor requires hours of research, meetings, conference calls, and dialog with the investigators and prosecutors. AOL personnel perform pre-trial litigation support, custodian of records, nexus, as well as fact and expert witness testimony to assist the government. Frequently, two or more AOL employees are usually out of the office offering testimony in jurisdictions all over the United States. Many prosecutors have reported that their success at convicting computer/Internet related criminals would not have been possible without the assistance and testimony from AOL records, fact, and/or expert witnesses.

AOL devotes considerable resources to these efforts. While AOL does not provide its assistance for recognition, it has received numerous awards, commendations, and citations from the US government. Those include: the United States Department of Justice Commendation Award - October 1997; High Technology Crime Investigation Association Award - March 1999; Federal Bureau of Investigation - Exceptional Service in the Public Interest Award - March 2000; Federal Bureau of Investigations White Collar Crime Program Award and Special Recognition for Outstanding Support - April 2001; National Missing and Exploited Children's Award - May 2001, May 2002 and May 2003; Computer Crime and Forensics Symposia Excellence Award - August 2001; United States Department of Justice/National Missing and Exploited Children's Individual Corporate Award, 2004. United States Secret Service Award for Outstanding Service in the Public Interest, 2004; FBI and United States Department of Justice Award for its role in the International Online Child Sexual Victimization Symposium, 2004.

Although AOL has taken a leadership role in the development of best practices and solutions, we recognize that as technology evolves and criminals become more sophisticated, much more needs to be done. It is also clear that many members of this Committee are very concerned about protecting children and want more to be done. As it has in the past, AOL aims to rise to these new challenges and has developed a proposal to address these concerns in the most effective manner.

Specifically, AOL commits to: (1) voluntarily preserve all relevant records relating to a report by an ISP to NCMEC; (2) support a legislative grant of authority to NCMEC to send preservation letters to ISPs upon review and determination that the referred images are child pornography; (3) build and expand upon AOL's digital signature technologies and to share it with other industry colleagues to expand its reach; (4) investigate new and innovative technologies to make the Internet a dangerous place for predators but not legitimate users; and (5) most important, work with law enforcement to identify tools that will assist them in their critical work.

As a demonstration of our commitment, AOL has organized and joined with a team of companies, including Earthlink, Microsoft and Yahoo!, which are here today, to

develop effective technologies to investigate and prevent child pornography online and also to provide financial and personnel resources to NCMEC to further these efforts. These measures will ensure that law enforcement has all of the necessary data resources and tools so that they can pursue a successful investigation.

I am aware of the ongoing discussions between the Department of Justice and industry concerning the merits of a statutory mandate requiring that ISPs retain large amounts of data about the user's activity online for up to 2 years. I believe that a careful assessment of these proposals will show that they are in fact counterproductive and the efforts to create this massive and costly database will fall far short of its intended goal. Warehousing of data requires the allocation of enormous resources to maintain and secure that data. Those resources would be better focused on supporting law enforcement in the investigation of real-time active cases. Additionally, creating such a voluminous database will actually frustrate law enforcement's goal of locating and identifying the suspects they are pursuing. As databases grow in size and complexity the risk of data corruption increases as well. As a result, the possibility of not finding the requested information increases as does the potential for a false match.

Finally, even the best efforts at creating these massive databases are destined to fall short of their desired goal because they are easily circumvented. There are thousands of Internet access points that would not be covered by this data retention net, including Universities and other academic institutions, libraries, governments, the military, employers, and tens of thousands of wireless hotspots. A determined predator need only utilize one of these services to avoid the net.

AOL has long partnered with law enforcement in combating online offenses against minors and we recognize that law enforcement has a critical role to play in dealing with the use of the Internet to victimize children. However, AOL believes that the best strategies and solutions for solving the crises of child pornography and child predation lie with technology companies such as those testifying before you today.

In closing, we are committed at AOL to dedicate whatever resources are necessary to create a safe and secure medium for our most vulnerable users: children. We look forward to working with the Committee, the Department of Justice, and other stakeholders to ensure that no child is victimized by the abuse of our medium.

# # # # #

MR. WHITFIELD. Well, Mr. Ryan, thank you.

And I would remind all of the witnesses that we do have your testimony, and we would urge you to try to stay within the 5-minute rule. And thank you very much for your testimony.

Mr. Baker.

MR. BAKER. Chairman Whitfield, Ranking Member Stupak, members of the subcommittee, I am Dave Baker, Vice President for Law and Public Policy with EarthLink.

Thank you for inviting me to testify today as you continue to examine the critically important issue of how we all can make the Internet safer for our children. The Internet is a tremendous resource. As a father, I marvel at my own children's ability to use the Internet to help them with their homework, to challenge them with knowledge that supplements what they learn in school, and to satisfy their genuine intellectual curiosity.

At EarthLink, we are proud to have worked for over 12 years to develop this important tool for learning, e-commerce, and legitimate communications and entertainment. And we have worked hard to combat each new public threat as it has arisen, including spam, spyware, and phisher sites. We are similarly engaged in an ongoing battle against those who would use the Internet to harm our children.

There is no question that the Internet's capabilities provide criminal predators with new ways to attack children. The stories you have brought to light are chilling. Criminals, and they are just that, abusing children and then putting pictures of that abuse online. These are perverse and unlawful acts for which we should have no tolerance.

At EarthLink, we try to provide our subscribers with as safe as possible an environment for children to gain the benefits of the Internet while minimizing the risks. We focus on three strategies: one, prevention, empowering parents with strong parental controls and safeguarded communications tools; two, reporting, getting information on suspected child pornography and other abuse to the National Center for Missing and Exploited Children; and three, enabling prosecution, responding to law enforcement requests for data to assist the investigation and prosecution of abusers.

I will discuss each of these in further detail.

The first of our three strategies is prevention. Our website contains family safety information, such as the Kids Fighting Chance: 50+ Safety Tips, which EarthLink promotes in partnership with the Federal Bureau of Investigation. EarthLink is also proud to serve on the Steering Committee of GetNetwise, an alliance of industry and public-interest organizations, which provides tips on safe Internet usage, lists of family-friendly websites, information on parental controls, and links to report trouble if it is found. Our free downloadable parental controls give

parents options as to what access to permit their children to have to the Internet and what access to permit others to have to their children. For web surfing, parents can use parental controls to specify whether they want their child to be limited to a white list of 15,000 EarthLink-approved websites or to be permitted to go anywhere other than sites EarthLink specifically blocks.

In addition, parents can customize these lists. Even for those websites not specifically blocked, EarthLink's parental controls automatically check all webpage a child visits and remove inappropriate language before displaying them. In addition, children cannot create blogs when parental controls are activated. For e-mail and instant messaging, parents can use the Cyber Friends feature of our parental controls to create an approved list of persons that his or her child can contact. If the child is e-mailed by or attempts to e-mail someone who is not on the approved list, the e-mail is blocked and stored until the parent can review it. Parents can also specify whether their child can open attachments.

For parents of younger children, we provide the Kids Patrol browser, which includes its own filtered web browser, e-mail, chat, bulletin board, and instant message programs. Our parental controls also allow parents to limit the time of day and the total number of hours per day, week, or month their children may spend online. With these services, we work to empower parents to supervise and protect their children's online use.

Finally, I note that while EarthLink does not operate its own chat rooms or provide social networking services, as more Web content is produced by individual users, the challenges facing all of us are greater.

The next step is reporting. Beyond prevention, we also report and facilitate the reporting of unlawful child exploitation to the National Center for Missing and Exploited Children, NCMEC. If a customer discovers suspected child pornography, they can e-mail complaints to [abuse@EarthLink.net](mailto:abuse@EarthLink.net). In addition to handling customers' reports of fraud, spam, and other violations of our acceptable use policy, when one of our abuse investigators receives a complaint about child pornography, the investigator immediately reports that information to NCMEC's CyberTipline. Customers may also call us with complaints about suspected child pornography. All of our customer service representatives are specifically trained and given written guidance on how to facilitate the reporting of child pornography to NCMEC.

As mentioned by Mr. Ryan, EarthLink is also proud to ban together with AOL, Yahoo!, Microsoft, and America Online to fund a new Center for Child Protection Technologies within NCMEC to develop technological solutions to combat online child abuse.



Prosecution. Finally, EarthLink cooperates with law enforcement investigations and prosecutions of child exploitation cases. We regularly receive subpoenas requesting subscriber information, such as when a customer uses a specified IP address at a given date and time or which customer is associated with a particular username. We retain this information in a readily-accessible live database for several months and then archive it in searchable and retrievable tape storage for several years. We receive approximately 1,000 subpoenas per year, approximately 15 percent of which involve allegations of child exploitation. We give legal process associated with child endangerment or exploitation the highest priority.

In conclusion, we believe that a combination of the proper use of prevention tools, like parental controls, the prompt reporting of allegations of child exploitation, and cooperation with law enforcement investigations and prosecutions can help make the Internet a safer place for children and their families.

Thank you again for the opportunity to testify on this important matter.

[The prepared statement of David Baker follows:]

PREPARED STATEMENT OF DAVID BAKER, VICE PRESIDENT, LAW AND PUBLIC POLICY,  
EARTHLINK, INC.

Chairman Whitfield, Ranking Member Stupak, Members of the Subcommittee, on behalf of EarthLink, Inc., thank you for inviting me to testify today as you continue to examine the critically important issue of how we all can make the Internet a safer environment for our children. The Internet is a tremendous resource for children. As a father, I marvel at my own children's ability to use the Internet to help them with their homework, to challenge them with knowledge that supplements what they learn in school, and to satisfy their genuine intellectual curiosity. At EarthLink, we are proud to have worked for over twelve years to develop this important tool for learning, e-commerce and legitimate communications and entertainment. And we have worked hard to combat each new public threat as it has arisen – including spam, spyware and phisher sites. We are similarly engaged in an ongoing battle against those who would use the Internet to harm our children.

There is no question that the Internet's capabilities provide criminal predators with new ways to attack children. The stories you have brought to light are chilling. Parents abusing their own children and then putting the pictures of that abuse online. Criminals – and they are just that – luring children into performing lewd acts to be

recorded and shared. These are disgusting, perverse and unlawful acts for which we collectively should have no tolerance.

At EarthLink, we try to provide our subscribers with as safe as possible an environment for children to gain the benefits of the Internet, while minimizing the risks. We focus on three strategies:


- Prevention – Empowering parents with strong parental controls and safeguarded communications tools;
- Reporting – Getting information on suspected child pornography and other abuse to the National Center for Missing and Exploited Children;
- Enabling prosecution – Responding to law enforcement requests for data to assist in the prosecution of abusers.

To each of these strategies we bring our proven track record for combating anti-consumer abuses. I will discuss each of these in further detail.


Before I do so, however, let me give you a little background on EarthLink. For twelve years, EarthLink has been on the cutting edge of delivering the Internet to American consumers and business, first through dial-up, then broadband and now VoIP, wireless voice and municipal wireless Internet services. We were an early provider of premium dial-up Internet access, and we also popularized value dial-up through our PeoplePC brand. Over the past twelve years, we've seen the Internet grow from the specialized province of a few tech-savvy early adopters to an integral part of American work and family life. As of the end of the first quarter 2006, EarthLink had approximately 3.4 million dial-up subscribers and 1.7 million broadband subscribers, giving us about 3.7% of total broadband subscribers nationwide.

**I. Prevention.**

As I mentioned, the first of our three strategies is prevention. We are not a Bell company or a cable company. We make our business by providing our customers with a more customer-friendly Internet experience. Our motto is, "We revolve around you." So we have developed and incorporated into our service offerings the EarthLink Protection Control Center which contains tools to fight spam, spyware, pop-ups, hackers, & viruses. Our website also contains family safety information such as the Kids Fighting Chance 50+ Safety Tips (available at [www.earthlink.net/software/free/parentalcontrols/tips/](http://www.earthlink.net/software/free/parentalcontrols/tips/)), which EarthLink, working in partnership with the Federal Bureau of Investigation and Kids Fighting Chance, promoted in 2004 in 33 malls in 26 cities across the country. And our free, downloadable Internet safety tool package (called EarthLink Total Access) includes our Parental Controls.


[myEarthLink](#) | [Web Mail](#) | [My Account](#) | [Support](#) | [mySecurity](#)

[EarthLink](#)

powered by  


[HOME](#)
[INTERNET ACCESS](#)
[BUSINESS](#)
[VOICE](#)
[WIRELESS](#)
[SOFTWARE & TOOLS](#)
[MEMBER CENTER](#)
[CART](#)

**■ SOFTWARE & TOOLS**  
 ↓ **For Members**  
 Free  
 Premium  
 ↓ **For Non-Members**  
 Free  
 Premium


**■ HAVE A QUESTION?**  
**Get answers FAST!**  
 Not sure what service is right for you? Want to upgrade your service?  
 Click for live **SUPPORT CHAT**  
 Open 6am-12am EST Monday-Sunday  
 Need help with your current service?  
 Click for live **SUPPORT CHAT**  
 Open 24/7

**EarthLink® Parental Controls**  
**Top 50+ Kids Safety Tips from Kids Fighting Chance and EarthLink®**  
**Safety Tips for Kids Aged 5 to 11**

1. Always let parents know where you are going, who you'll be with, and what time you will arrive home.
2. Always get permission from a parent before going to someone's house.
3. Do not answer the door if you are home alone.
4. Never open the door to a stranger.
5. Never say you are home alone when answering the phone. (Instead say something like, "My dad is in the shower. Can I take a message?")
6. Never let someone from the cable company, phone company, or another uniformed person into the house if an adult/parent is not present.
7. Always lock the door when home and put on the alarm system (if one is available).
8. Never enter anyone's car unless a parent has said it is OK to do so.
9. Keep objects in each room that might be used as a weapon (like a baseball bat or walking cane).
10. Call local police or 911 to make sure they're telling the truth if someone claims to be a police officer.
11. Never take gifts or candy from strangers.
12. Never play in isolated areas or inside/near deserted buildings.
13. Always go with your instincts and go somewhere safe if you feel fearful of someone.
14. Call 911 in an emergency and say "I need help" or leave the phone off the hook if talking is not possible—the police can trace your location anywhere.
15. Never stop fighting back and always keep looking for an escape route.
16. Learn and practice the Fighting Chance™ techniques!

**■ LEARN MORE**  
**Parental Controls**

- [Quick Tour](#)
- [FAQ](#)
- [EarthLink Family Safety Advice](#)
- [Top 50+ Kids Safety Tips](#)
- [Download TotalAccess](#)
- [Join EarthLink](#)


[Visit the Kids Fighting Chance web site](#)

#### **Safety Tips for Kids Aged 12 and Older**

1. Call a parent to come anytime, anywhere, if you are in a situation where you feel uncomfortable (no matter how late or how far).
2. Never hitchhike.
3. Always avoid short cuts through alleys, deserted parks, or buildings.
4. Never walk alone—use the "buddy system".
5. Remember suspicious car license plates and write the plate number in snow or dirt if no pen or paper is available.
6. Trust your instincts—recognize and report suspicious behavior.
7. Give up jewelry or cash if attacked.
8. Always walk near lights and stay in public and open areas at night.
9. Learn and practice the Fighting Chance™ techniques!

#### **Safety Tips for Parents**

1. Raise your child to have a strong sense of self-respect and self-confidence.
2. Create an environment where your child feels free to talk and make time to listen to your child.
3. Talk about difficult topics with your child—uninformed children are the most vulnerable.
4. Teach your children to recognize danger signals or abduction scenarios (e.g., "Can you help me find my lost puppy?").
5. Know your child's friends and their parents.
6. Never leave children under 5 years old unattended.
7. Avoid clothing or toys with child's name on it.
8. Thoroughly check references of all potential babysitters or childcare workers.
9. Make sure your child has all appropriate phone numbers and emergency services numbers, post them in several places throughout the house.
10. Teach your child safe hiding places throughout the house.
11. Teach your child escape routes out of the house and places to run (e.g., neighbors' house).
12. Point out safe houses in your neighborhood that your child can go to if frightened or chased.
13. Never leave a child alone in a public place.
14. Always accompany your child into public restrooms.
15. Always go with your child to supervise door-to-door activities such as fundraising or Halloween.
16. Teach child that police are their friends.
17. Keep up-to-date medical and dental records of your child.
18. Have your child fingerprinted.
19. Find out where convicted sex offenders live in your community.
20. Learn the Fighting Chance™ techniques and practice them with your child!

#### Communication Tips for Parents

1. Make it a family rule that your child must let you know where they are at all times.
2. Choose a family "password" that children can use if they are ever in trouble. Review it every week.
3. Make sure your children know their last name, phone number, and address.
4. Make sure your child knows how to dial 911.
5. Let your child know it is all right to say "no" to an adult if asked to do something they are not comfortable doing.
6. Teach child that adults never need help from children for any reason (e.g., help find puppy, directions, etc).
7. Explain that if an adult or child ever asks them to "keep a secret" it is all right for them to discuss it with a parent/trusted adult.

#### Essential Escape Techniques

1. If taken by a stranger, teach to yell specific phrases such as, "Help, I have been abducted, I do not know this person!" "I need your help. I'm being kidnapped!"
2. If grabbed inside a public place like a mall, teach child to drop weight down, twist, stretch out, kick their legs, and scream "Help! I need your help. I'm being kidnapped!"
3. If child is grabbed in a store, teach child to yell for a cashier or other adult and to shatter merchandise and knock down displays. Tell child to try to grab onto the nearest person.
4. If forced into a car or building, teach child to scream and shatter objects.
5. If a car pulls up beside a child, teach your child to move away from the car. Tell child to run in the opposite direction the car is facing.
6. If abducted in a parking lot, teach child to run, pound on cars to set off car alarms, and to go under a parked car if possible.
7. If locked in a trunk, teach child to push out taillights and let wires dangle out.
8. If abducted in to a car, teach child to jump into the backseat and go out the back door.
9. If stuck in the front seat of a car, teach how to pull out wires under dashboard to disable car or put something small inside the ignition switch.
10. If locked in an apartment or house, teach child to always try all doors and windows for escape route. Create an emergency situation (flood bathroom, break windows, set off alarms).

To promote online safety, we begin by providing Online Safety Tips for both parents and children ([www.earthlink.net/software/free/parentalcontrols/advice/](http://www.earthlink.net/software/free/parentalcontrols/advice/)):

#### Online Safety Tips

##### Safety Tips for Parents

1. **Talk to your child:** Communicate openly with your children about the potential dangers of the Internet.
2. **Keep the computer in a common room:** The best place for a computer is in a common room in the house, not your child's bedroom. It is easier to make sure the wrong people are not communicating with your children if the screen is visible to you.
3. **Use parental control tools:** Most ISPs provide some form of parental control and blocking software. While these can be great tools, do not rely on them completely to protect your children.
4. **Monitor the chat rooms:** While electronic chat can be a great place for children to make new friends, it is also prowled by computer-sex offenders. Be sure you're familiar with your children's favorite chat rooms.
5. **Have a shared email account:** Always maintain access to your child's online account and randomly check his/her email.
6. **Teach responsibility:** The Internet is a great tool, and as a parent, you should teach your child responsible use of the resources online. There is much more to online experience than chat rooms.

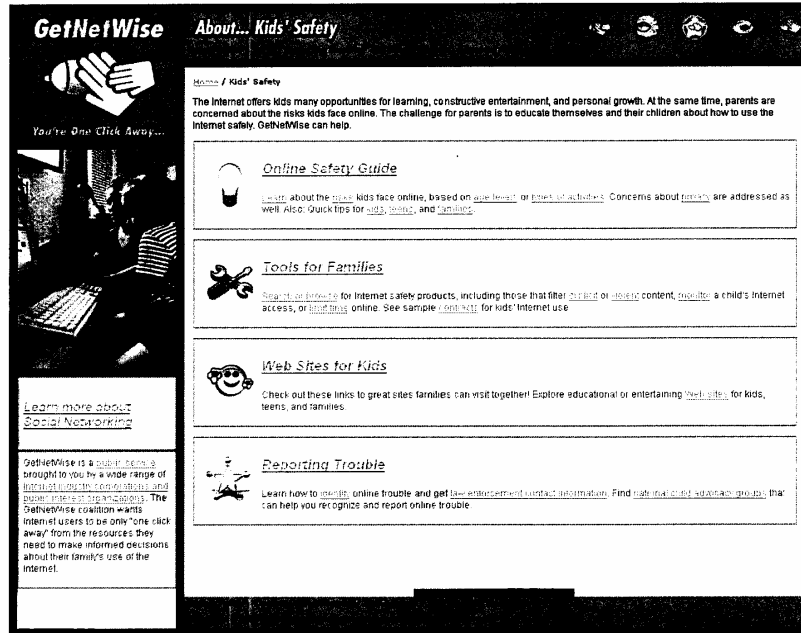
##### Safety Tips for Kids Aged 5 to 11

1. **Do not share personal information:** Never share any information such as a home or school address, telephone number, parent's work address/telephone number, or the name and location of your school without your parent's permission.
2. **Never agree to meet an online friend in person:** Never make plans to meet anyone you meet online without first checking with parents. If your parents agree to the meeting, be sure that it is in a public place and bring a friend or adult along.
3. **Never send your picture:** Don't send a person your picture or anything else without first checking with your parents.
4. **Don't respond to mean messages:** You shouldn't respond to any messages that are mean or make you feel uncomfortable in any way.

EarthLink is also proud to support and be on the steering committee of GetNetWise ([www.getnetwise.org](http://www.getnetwise.org)), a public service by Internet industry corporations and public interest organizations to help ensure that Internet users have safe and constructive online experiences. The GetNetWise website has materials that specifically address children's safety, the first page of which is shown below. As part of its Online Safety



Guide, GetNetWise provides safety information specifically related to different Internet settings, including social networking sites and Instant Messaging.



EarthLink's Parental Controls suite empowers parents to follow these safety recommendations, giving them options as to what access to permit their children to have to the Internet – and what access to permit other parties on the Internet to have to their children. Using our Parental Controls, parents can specify whether they want their child to be limited to 15,000 EarthLink approved sites (a “whitelist”), or to be permitted to go anywhere other than sites EarthLink specifically blocks (a “blacklist”). In addition, parents can customize these lists, adding to the list of approved sites their child may visit or the list of blocked sites the child may not visit. Moreover, even if a website is not specifically blocked by EarthLink or by the parent's request, EarthLink's Parental

Control software will automatically check the language on all web pages the child visits and remove inappropriate language before displaying them. If the number of inappropriate words on a web page is excessive, the Parental Control software will block the site altogether. In addition, children cannot create blogs when Parental Controls are activated.

Furthermore, using the CyberFriends feature of EarthLink's Parental Controls, a parent can create an approved list of persons that his or her child can e-mail, IM or chat with over the Internet. If the child is e-mailed by or attempts to e-mail someone who is not on the approved list, the e-mail is blocked and stored until the parent views the e-mail and decides whether the child can read it or deletes it. In addition, a parent can specify whether the child will be able to open attachments. CyberFriends strictly limits not only whom your child can contact, but also who can contact your child over the Internet.

## 1. Introduction

## 2. What You Can Control

## 3. Getting Started

## 4. Setting Up a Child Profile

## 5. My Account

## 6. Profile Settings

## 7. The KidPatrol Browser

## 8. Getting Help

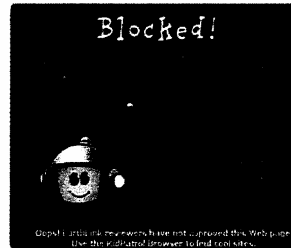
**EarthLink® Parental Controls****What You Can Control**

With Parental Controls, you can customize these Internet safety features for each of your children:

**Web Blocking and Filtering**

Limit your child's Web surfing to EarthLink's list of more than 15,000 kid-friendly Web sites, or let your kids visit all Web sites except for the 3 million sites that EarthLink has blocked. You can also create your own lists of approved and blocked Web sites.

Even if a site is not specifically blocked by you or EarthLink, Parental Controls can automatically check the language on all Web pages your child visits and remove inappropriate language before displaying them. If the number of inappropriate words on a Web page is excessive, Parental Controls blocks the site completely.

**CyberFriends**

CyberFriends are the people you allow your child to communicate with online. You create a list of approved pals—friends and family—so that you don't have to worry about your child being bothered by strangers. You can also define which features of the CyberFriends Communicator (email, chat, bulletin boards, instant messaging, etc.) your child can use.

**Email Screening**

If someone who is not a CyberFriend sends email to your child, Parental Controls locks that email so that you can review it first. You can then unlock the message so your child to see it, or simply delete it. Parental Controls also locks email that your child sends to non-CyberFriends; you can either unlock or delete those emails, too.

**Time Limits**

If you're concerned about your child spending too much time online, you can restrict the hours per day, week, or month that your child can use the Internet.

For parents of younger children, we provide the KidsPatrol Browser. In addition to providing a web browser function, the KidsPatrol Browser contains its own email, chat, bulletin board and instant messaging programs.

Our Parental Controls software also allows parents to set a time limit on a child's Internet usage, including limiting the precise times during each day when the Internet can be used or by limiting the total number of hours per day, week or month that a child may spend online.

We try to make these Parental Controls easy to use. They are downloadable for free as part of our standard Internet protection package. When adding a child's email to the parent's account, Parental Controls can be activated with simply a click of the mouse.

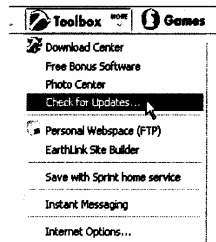
1. Introduction
2. What You Can Control
3. Getting Started
4. Setting Up a Child Profile
5. My Account
6. Profile Settings
7. The KidPatrol Browser
8. Getting Help

### EarthLink® Parental Controls

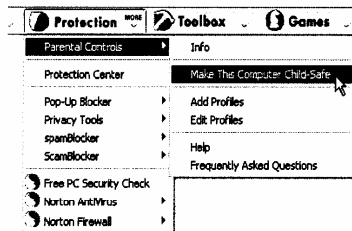
#### Getting Started

To use Parental Controls, you'll need the latest version of [EarthLink TotalAccess for Windows](#).

Using TotalAccess, you can download and install Parental Controls via the Update Manager, available under the **Toolbox** menu:



After Parental Controls are installed, you'll see new options under the **Protection** button in the Task Panel. Choose **Make This Computer Child-Safe** to require everyone in your household to sign in to TotalAccess before accessing the Internet. This prevents your kids from using other software to go online and bypassing Parental Controls:



Also, make sure the **Save** box in the TotalAccess sign-in window is unchecked for any parent profiles in your household. If you save your password, your children will be able to sign in under your profile and bypass Parental Controls.

Moreover, we have made it easy to enter the child's permitted CyberFriends and to activate the web controls.



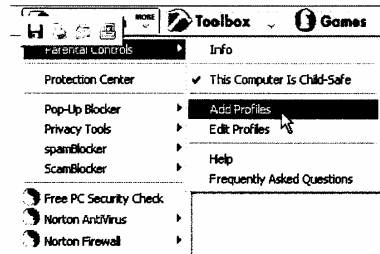
1. Introduction
2. What You Can Control
3. Getting Started
4. **Setting Up a Child Profile**
5. My Account
6. Profile Settings
7. The KidPatrol Browser
8. Getting Help

## EarthLink® Parental Controls

### Setting Up a Child Profile

Your next step is to create a profile for each child. This lets you customize Parental Controls to the needs of each child according to age. You can give your older kids more freedom to surf the Net while placing tighter restrictions on your younger children's online activities.

You can set up a profile from the Task Panel using the **Add Profiles** option:



You'll be taken to **My Account**, where you can create profiles (you'll have to sign in using your primary profile first).

Anytime you want to change the settings for a profile you've already created, go back to the Parental Controls menu in the Task Panel and choose Edit Profiles.

1. Introduction
2. What You Can Control
3. Getting Started
4. Setting Up a Child Profile
5. My Account
6. Profile Settings
7. The KidPatrol Browser
8. Getting Help

## EarthLink® Parental Controls

### My Account

The Parental Controls page at **My Account** is where you manage your kids' safety profiles. It lists all the profiles in your account:

To create a profile, click **Add a New Profile**. To change an existing profile, click the **Edit** link in a child's profile and look for the **Parental Controls** section on the child's profile page:

Profile #3		Delete
	Status	Options
Name	Janet Doe	<a href="#">Edit</a>
Email Address	child2@earthlink.net	<a href="#">Edit</a>
Password	*****	<a href="#">Edit</a>
Parental Controls	ON	<a href="#">Turn OFF</a> <a href="#">Edit Settings</a>

Click **Edit Settings** to customize this child's profile. (You can turn Parental Controls on or off here, too.)

1. Introduction
2. What You Can Control
3. Getting Started
4. Setting Up a Child Profile
5. My Account
6. Profile Settings
7. The KidPatrol Browser
8. Getting Help

## EarthLink' Parental Controls

### Profile Settings

When you edit the Parental Controls settings for a child's profile, you choose which EarthLink features your kids can use, which Web sites they can see, who they can talk to, and how long they can stay online:

### Parental Controls

[Sign Out](#)

#### Menu

[My Account Home](#)  
[Profiles](#)  
[Service Details](#)  
[Help](#)

#### Parental Controls

[Profile Settings](#)  
[Parental Controls Info](#)  
[Download TotalAccess Software](#)

#### Profile Settings

If you want to change another child's profile, [click here](#).

If your child is on the Internet right now, he or she **MUST** sign out of TotalAccess and sign in again for any changes to take effect (right-click on the EarthLink icon at the bottom of their screen, near the clock, and select Sign Out.)

#### Profile - Janet Doe

Email Address: child2@earthlink.net

Parental Controls: Enabled

Gender:

Date of Birth:

Age Group:

Restore this profile to the default settings for the selected age group.

[Restore This Profile](#)

[Learn More](#)

#### Web Browser Settings

You have two options for limiting your child's Web browsing. You can restrict them to visiting a list of **Approved Sites**, or allow them to visit any site except **Blocked Sites** (you can add sites to either list).

You can also require that younger children use the EarthLink KidPatrol Browser, which has clear child-friendly navigation and colorful special effects.

Finally, you can have EarthLink Parental Controls scan the Web pages your child visits - masking or blocking inappropriate content.

[Web Browser Settings](#)

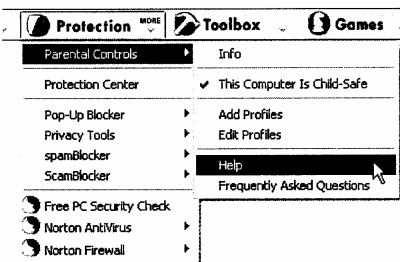
EarthLink Parental
Tour

1. Introduction
2. What You Can Control
3. Getting Started
4. Setting Up a Child Profile
5. My Account
6. Profile Settings
7. The KidPatrol Browser
8. Getting Help

## EarthLink Parental Controls

### Getting Help

If you ever need more information about using Parental Controls, help is available from the TotalAccess Task Panel:



The screenshot shows a software interface with three main tabs: 'Protection', 'Toolbox', and 'Games'. The 'Protection' tab is active and has a dropdown menu open. The menu items are: 'Parental Controls' (with a right arrow), 'Protection Center', 'Pop-Up Blocker', 'Privacy Tools', 'spamBlocker', 'ScanBlocker', 'Free PC Security Check', 'Norton AntiVirus', and 'Norton Firewall'. The 'Parental Controls' dropdown is further open, showing 'Info', 'This Computer Is Child-Safe' (with a checkmark), 'Add Profiles', 'Edit Profiles', 'Help' (highlighted by a mouse cursor), and 'Frequently Asked Questions'.

Now that you know the basics of how Parental Controls work, you're ready to make the Internet safe for your kids. Install Parental Controls today-and enjoy peace of mind!

With these services, we have worked to empower parents to supervise and protect their children's online use. Finally, I note that EarthLink does not itself operate general IM services (*i.e.*, other than the KidsPatrol IM), nor does it operate its own chat rooms or provide "social networking" services.

## II. Reporting.

Moving beyond prevention, our next strategy is to report and to facilitate the reporting of unlawful child pornography. As is our obligation under law, when EarthLink discovers material that it believes may be child pornography, it reports that material to the National Center for Missing and Exploited Children (NCMEC), and has



done so since 2001. In our experience in the ordinary conduct of our business, we have not discovered substantial amounts of child pornography.

There are generally two ways that we receive complaints. The first is through customer e-mail complaints to our various abuse channels (such as [abuse@earthlink.net](mailto:abuse@earthlink.net)). Our Abuse team regularly handles customers' reports of fraud, spam and any other violations of EarthLink's Acceptable Use Policy. When one of our abuse investigators receives a complaint about material that appears may be child pornography, the investigator immediately reports that allegation to the National Center for Missing and Exploited Children's CyberTipline.

We may also receive complaints about suspected child pornography or exploitation through calls to our customer service representatives. All of our customer service representatives are specifically trained and given written guidance on how to walk a customer through the steps of reporting child pornography to NCMEC. This written guidance is automatically available to them as they are answering calls. This results in the complainant forwarding the offending material or related information directly to NCMEC.

Our Abuse team also maintains regular contacts with the security staffs of other ISPs. Through this network, we would be notified by other ISPs if they found that an EarthLink subscriber was sending out prohibited child pornography. We can then conduct a follow-up investigation and take appropriate action. In our experience, this happens 2-3 times per year, with resulting referrals to NCMEC. If it comes to our attention that a site we are hosting has child images, we immediately contact law enforcement.

**III. Enabling Prosecution.**

EarthLink fully cooperates with law enforcement investigations and prosecutions of child exploitation cases. We regularly receive subpoenas requesting specific subscriber information, such as which customer used a specific IP address at a specific time, or which customer is associated with a particular username. EarthLink receives approximately 1,000 subpoenas per year, approximately 15% of which involve child exploitation. We give legal process associated with child endangerment or exploitation the highest priority.

We retain the information necessary to provide police and prosecutors with information such as which user was assigned a given IP address at a given date and time. These logs are kept in a readily accessible "live" database for several months and are then archived in searchable and retrievable tape storage for seven years.

As further evidence of this, let me relate a recent experience we had. In November 2005, EarthLink received a subpoena for subscriber information for IP addresses, some of which were over five months old. We were able to pull the necessary back-up tapes from archives, retrieve the information and respond to law enforcement within two weeks, notwithstanding the intervening Thanksgiving holiday. We stand ready, willing and able to promptly assist law enforcement authorities when they need such assistance to help put criminals behind bars.

\* \* \*

In conclusion, we believe that a combination of the proper use of prevention tools like Parental Controls, the prompt reporting of allegations of child exploitation, and cooperation with law enforcement prosecutions of offenses can help make the Internet a

safer place for children and their families. Like everyone here today, we would much rather help prevent child pornography and exploitation than to deal with the aftermath. Thank you again for the opportunity to testify today on this important matter.

MR. WHITFIELD. Thank you, Mr. Baker.  
And Ms. Banker, you are recognized for 5 minutes.

MS. BANKER. Chairman Whitfield, Ranking Member Stupak, and members of the subcommittee, thank you for the opportunity to address the important topic of protecting children online.

My name is Elizabeth Banker. I am Vice President and Associate General Counsel for Yahoo!. For the past 7 years, I have managed Yahoo!'s Law Enforcement Compliance Team. During my time at Yahoo!, I have personally reviewed and reported child pornography, helped design our NCMEC reporting process, and responded to emergency calls from law enforcement to help find missing and abused children. I can tell you that Yahoo! has a long history and a deep commitment to making the online environment safer for children. We have done this by: one, building safer online spaces; two, identifying and removing users who engage in illegal conduct involving children; and three, working with NCMEC, law enforcement, and our industry peers.

Let me describe these efforts.

Yahoo! was an early leader in creating child-friendly spaces online. Ten years ago, we launched Yahoo!igans, a mini version of Yahoo! that is a safe place for kids. More than four million unique users each month use Yahoo!igans for news, music, and games.

We also work to protect children on our other services. We have put in place a series of age restrictions so that parts of our network, like Yahoo! Chat, are off limits to children registered as under the age of 18. We have even tighter restrictions for children under 13 who may not create a profile or play games at Yahoo.com.

We also provide filtering, blocking, and parental control tools. Parents who use Yahoo!, through our broadband partners, can restrict children's activities both on and off of our network. For other users, we offer Safe Search to exclude adult content from responses to search queries. In addition, we provide tools to filter offensive language and to block and ignore unknown users or offensive communications. And Yahoo!'s Family Resource Center offers parents user-friendly information on these tools and other educational resources.

Yahoo! has policies and technology to help identify violators using our network to engage in illegal behavior. We have strict terms of service that prohibit harmful and abusive conduct, and we provide tools to enable users to report violations. For example, we have built report abuse links into Yahoo! Chat and webcam. When users report abuse, we review the reports, shut down violators' accounts, and escalate appropriate reports to NCMEC. We also take affirmative steps to detect and remove child pornography through technology, such as filters and algorithms, as well as through human review. Each of these is tailored to our specific services.

We work closely with NCMEC and law enforcement to ensure that online child predators and child pornographers are promptly identified, investigated, and prosecuted. We have invested significant resources to develop effective systems for reporting child pornography, and we meet regularly with NCMEC to find ways to make our reporting more effective for law enforcement. For example, if child pornography is found on Yahoo! Groups or Yahoo! Photos, we can now report the IP addresses of the user who originally uploaded it. Law enforcement has said that our capability has been very helpful in their investigations.

In addition, we work closely with the United States Internet Service Provider Association, or USISPA, and NCMEC to develop a set of sound reporting practices for ISPs. Yahoo! supports law enforcement within the framework required by law and our commitment to the privacy of our users. Our compliance team is available 24/7 to respond to legal process. All child endangerment cases are given priority. We provide a manual to assist law enforcement with their investigations, and we train law enforcement personnel who focus on protecting children, such as the Internet Crimes Against Children Task Force. Also, we provide NCMEC millions of dollars of public service advertising placements on the Yahoo! network.

While we are proud of our progress, we recognize that there is more work to be done. One recent change that we have made builds on the success of Yahoo! UK's partnership with the Internet Watch Foundation, or IWF. We are now removing child pornography sites on IWF's list from our U.S.-based search results as well as from Yahoo! UK.

But the issue of child safety is bigger than any one company. I would like to describe two new industry initiatives that we support.

First, Yahoo! supports the USISPA proposal authorizing NCMEC to issue preservation letters to ISPs. This will eliminate the delays between when ISPs report and law enforcement issues preservation requests.

Second, all ISPs should follow USISPA's Sound Practices for Reporting to NCMEC. Today, Yahoo! and certain major ISPs adhere to these practices, but others do not. If other ISPs follow these practices, law enforcement could better pursue cases referred to NCMEC and not just the cases from a select few providers.

Finally, I would like to highlight our announcement today with NCMEC, AOL, Microsoft, EarthLink, and United Online. Together, we are launching an aggressive campaign against child exploitation on the Internet through a new Center for Child Protection Technologies. Through this center, industry leaders will come together to develop and deploy technological solutions to disrupt predators' ability to use the Internet to abuse children. Our industry peers are invited to join this effort.

Mr. Chairman, Yahoo! believe that our actions make our network safer for children, and the proposals I have described will make it more likely that violators will be identified, investigated, and punished. We at Yahoo! look forward to working with members of the subcommittee in the ongoing battle to keep children safer online.

Thank you for the opportunity to testify today.

[The prepared statement of Elizabeth Banker follows:]

PREPARED STATEMENT OF ELIZABETH BANKER, ASSOCIATE GENERAL COUNSEL, YAHOO!  
INC.

**Introduction**

Chairman Whitfield, Ranking Member Stupak, and Members of the Subcommittee, thank you for the opportunity to address the Subcommittee on the important topic of protecting children online. My name is Elizabeth Banker. I am Vice President and Associate General Counsel at Yahoo!, where I have managed the law enforcement compliance function for the past seven years. The compliance team consists of dedicated professionals whose primary function is to respond to legal process with respect to information about subscribers, and to report instances of child pornography to the National Center for Missing and Exploited Children ("NCMEC"). From these experiences, I can tell you that Yahoo! has an unwavering commitment to promote online safety and that I personally, along with the rest of the Yahoo executive team, share the same commitment. In my time at Yahoo!, I have also seen how much the Internet generally, and Yahoo!'s services specifically, are used to provide information, education, and fun to children who would otherwise not have access to these opportunities to enrich their lives.

**About Yahoo!**

Yahoo! is one of the leading global Internet brands and one of the most visited Internet destinations worldwide. More than 411 million unique users worldwide visit Yahoo! each month. We offer a broad range and deep array of over 50 products and services that are designed to provide our users with the power to connect, communicate, create, access, and share information online. Many of our services are free to users. Unlike many service providers represented here today, Yahoo! does not provide users with internet access. Users may access Yahoo! using any mode of internet access available to them, whether through our partners Verizon and AT&T, through a dial-up connection, via a wireless connection in a coffee shop, or on their mobile phone.

**Yahoo! is Committed to Protecting Children Online**

Yahoo!'s commitment to fostering a safe online environment for users of all ages begins with our own products and services. Yahoo! actively works to prevent people from abusing our service in a way that harms children. As you may know, there are many different ways to protect children online including: (1) building safer, child-appropriate online environments; (2) implementing policies and tools to assist in reporting users who engage in inappropriate or harmful behavior; (3) deterring and detecting use of systems to distribute illegal child pornography; and (4) working with law enforcement to combat online exploitation of children and to ensure that people who use the Internet to sexually abuse children are promptly identified, investigated and prosecuted.

As I will describe in more detail, Yahoo! uses all of these techniques to help create a safer online experience for all users. We also actively engage with others who are critical partners in the effort to combat online exploitation of children, such as the Department of Justice, NCMEC, the Internet Crimes Against Children Task Forces, non-profit organizations that promote online safety, our peers in the industry, and our users. Yahoo! has an especially long history of creating child-friendly online spaces, working with NCMEC, and working with law enforcement agencies on issues related to child sexual abuse. We continue to build on our prior successes and to move forward with additional measures that will enhance online safety for children.

**How Yahoo! Makes Safer Places Online for Children**

Yahoo was an early leader in creating child-friendly spaces online. In 1996, Yahoo! launched Yahoooligans!, one of the first online resources of safe and child-appropriate Web sites. Yahoooligans! is a safe place to be a kid on the Internet. It is a mini version of Yahoo! that is



designed for children, but also has a variety of resources for parents and teachers. All websites and content listed in the Yahoo!igans! directory have been reviewed and approved by a trained staff of Yahoo! employees who are former teachers and librarians. Product offerings on Yahoo!igans! include news, music, movies, e-greetings, jokes, science, and close to 100 kid-safe games. Yahoo!igans! has more than 4 million unique users each month and was very proud to have won the Wired Kids Award in 2002.

Yahoo! also takes several measures to protect children who use services offered on Yahoo.com. One of these measures is to block younger users from using Yahoo! services that are likely to be used for grown-up interactions, such as Chat. Based on the birthdate provided upon registration, user accounts under the age of 18 are not currently allowed to participate in Yahoo! Chat or Yahoo! 360, Yahoo!'s social networking community. Similarly, children who are under the age of 13 may not register for a public profile as a Yahoo! user, participate in Yahoo! Games, or use Yahoo! Geocities to post a personal webpage.<sup>1</sup>

Yahoo! also helps children stay safe online by promoting the use of filtering, blocking, and parental control tools. We make available a parental control product to users of Yahoo! who have broadband Internet access through our partners such as Verizon and AT&T. Using parental controls, parents can filter or restrict their children's activities online, even when their children are trying to access sites that are off the Yahoo! network. These programs provide a robust mechanism for parents to oversee their children's online activities. For parents whose children access Yahoo.com through other providers, Yahoo! has a feature called "SafeSearch," which, when activated, is intended to prevent adult content from being displayed in response to search queries made by that user's Yahoo! account. In addition to SafeSearch, Yahoo! provides users with a number of features that allow them to customize their online experience, including tools to

---

<sup>1</sup> For more details on age-specific restrictions, see <http://help.yahoo.com/help/us/family>.

filter offensive language, set privacy preferences to block out conversations from unknown sources, and “ignore” specific users so they can stop receiving communications from anyone who harasses or offends them. Yahoo! educates its users on all of these features at a central site called our “Family Resource Center,” which can be found at <http://family.yahoo.com>. At our Family Resource Center, we also share safety and other helpful information and tools from our partners and other third party resources, such as NCMEC’s Netsmartz and GetNetWise.

#### **Yahoo’s Efforts to Block, Screen and Report Abuse**

Yahoo! has made a strong commitment to prevent illegal and/or abusive content on our networks. In addition to taking down illegal child pornography that is reported to us, we also enable users to report unwanted conduct to Yahoo! easily, report unlawful conduct involving children to NCMEC, and take affirmative steps to detect and remove child pornography from the Yahoo! network.

First, Yahoo! has strict Terms of Use and Community Guidelines that prohibit a wide range of harmful and abusive conduct, including any conduct that could harm minors. Second, Yahoo! has implemented a number of tools to make it easier for users to report violations of these policies, along with other types of unwanted and unwelcome interactions on the Yahoo! network. For example, Yahoo! has built a “report abuse” link into the frame of Yahoo! chat windows, webcam windows, and throughout the Yahoo! 360 service. “Report abuse” pages can also be found through Yahoo! Help. Users who see or receive illegal or unwanted communications can use these links to report the misconduct to Yahoo!. Under Yahoo!’s internal procedures, reports are reviewed, accounts of violators are shutdown, and reports that indicate any activity involving child pornography or solicitation of a minor are given special handling. Such reports are escalated for reporting to NCMEC, as appropriate. Moreover, in order to make our customer reports more effective for NCMEC and law enforcement, Yahoo!

has engineered special tools to allow the exact nature of the reported interaction to be brought to the attention of the customer care agent, and may be subsequently available to law enforcement if a criminal referral is made. As evidence of our serious commitment to protecting children online, Yahoo! continues to implement these tools and policies into new products and services.

Third, Yahoo! also takes affirmative steps to detect and remove child pornography from the Yahoo! network. We have devoted resources to develop technical tools, which are used in conjunction with human resources to detect and deter illegal child pornography. Our targeted, multi-faceted approach combines technology, such as filters and algorithms, with customer reports and human editorial input. These methods are customized for, and targeted to, specific Yahoo! services in order to be as effective as possible.

#### **Yahoo!'s Work with NCMEC To Improve the ISP Child Pornography Reporting Process**

Perhaps most importantly, Yahoo! has a long history of working closely with NCMEC to continuously refine the child pornography reporting process and to help NCMEC accomplish its mission of preventing child abduction and sexual exploitation, finding missing children, and assisting victims of child abduction and sexual exploitation. To that end, Yahoo! has invested significant financial and human resources in developing systems for reporting child pornography to NCMEC and law enforcement. Beyond merely reporting a minimum amount of information to NCMEC, Yahoo! has proactively teamed with NCMEC to optimize the ability of law enforcement agencies to find and prosecute pedophiles. We meet regularly with NCMEC personnel to discuss reporting procedures, and have made specific technical changes to our products and services to better protect children online.

One particular example of such an improvement involves Yahoo!'s changing its systems to enable Yahoo! to report IP addresses of users who upload child pornography images to Yahoo! Groups and Yahoo! Photos. This was done in order to be able to provide information to

NCMEC that would enable NCMEC to make a speedy referral to the appropriate law enforcement entity and to allow that law enforcement entity to act on illegal conduct as quickly as possible. We also deactivate users who have been the subject of NCMEC reporting.

In addition, we have worked closely with other service providers through the United States Internet Service Provider Association (US ISPA) and with NCMEC to develop a set of Sound Reporting Practices for ISPs, which we follow. The Sound Practices fill an important gap in the law by establishing guidelines for service providers on what an appropriate report of an incident of child pornography should contain.

Yahoo is also a member of the Financial Coalition Against Child Pornography, a coalition of leading banks, credit card companies, Internet service companies, NCMEC, and the International Center for Missing and Exploited Children (ICMEC).<sup>2</sup> The Coalition's goal is to make it impossible to profit from selling child pornography within two years by sharing information about websites selling child pornography, and stopping any payments passing to those sites.

I would also like to note that Yahoo!'s support of NCMEC extends well beyond the area of child pornography reporting. Yahoo! participates in Amber Alerts, sponsors NCMEC's annual Hope Awards and Congressional Breakfast, hosts a micro-site for NetSmartz on Yahoo!igans!, and provides NCMEC sponsored search and other advertising placements on the Yahoo! network.

#### **Yahoo! and Law Enforcement**

In addition to working with NCMEC, Yahoo! supports law enforcement in child pornography investigations in a number of different ways within the framework of our Terms of

---

<sup>2</sup> The Coalition consists of 19 entities, including America Online, American Express, and PayPal.

Service, our privacy policy, and the trust of our users worldwide. First, Yahoo!'s compliance team is available 24 hours a day, 7 days a week to handle emergencies and respond to subpoenas, search warrants, and court orders. All alleged child exploitation cases are given priority handling.

In addition to conducting frequent training for its own compliance personnel, Yahoo! also provides information and training to law enforcement agencies. Yahoo! has created a Law Enforcement Compliance Manual to ensure that law enforcement personnel are familiar with Yahoo!'s policies, procedures, and systems, and clearly understand how to obtain the appropriate investigatory information in child exploitation cases. We have also trained law enforcement personnel who focus on protecting children (such as Internet Crimes Against Children (ICAC) investigators and child exploitation prosecutors) regarding the function and operation of Yahoo! systems. We regularly participate in and/or sponsor a number of law enforcement training events, including the National ICAC Conference in 2005 and 2006, the San Jose ICAC Conference in 2004, 2005 and 2006, and this year alone, four events for the American Prosecutor Research Institute. Yahoo! is also a member of the Virginia Attorney General's Youth Internet Safety Task Force.

#### **Yahoo!'s Ideas for Building On Our Success Going Forward**

While we are proud of the progress we have made on our network and working with our partners, we recognize that there is more work to be done to combat illegal activity against children online. We will continue our efforts on several fronts, by improving user education and outreach about safety, including safety features in our products and services, refining our internal processes for combating child pornography, and strengthening our relationships with key partners like NCMEC.

Let me tell you about one recent change: building on the success of Yahoo! UK's partnership with the Internet Watch Foundation (IWF), Yahoo! is taking steps to implement elements of the IWF process for our US-based service. The IWF manages and controls a database of URLs which IWF analysts have determined to be illegal child abuse images. Using that database, the IWF notifies companies in the UK who host URLs where illegal material is posted, and simultaneously notifies law enforcement. For sites not hosted in the UK, the IWF shares the list with UK service providers so that they can remove the URLs from their search services or take other appropriate measures. As of June 2006, Yahoo! is removing sites on the IWF list from both the Yahoo! UK and Yahoo.com search results.

There are two other specific areas where we think concrete advancements can be made in the fight to eliminate child pornography and child exploitation. First, Yahoo! supports the US ISPA proposal that NCMEC be authorized to issue preservation requests to Yahoo! and other ISPs. This would remedy the most glaring gap in current child pornography investigations. Currently, only government entities may issue mandatory requests for preservation of data under 18 U.S.C. 2703(f). The lack of preservation authority for NCMEC can result in a substantial delay between the time the ISP first reports child pornography to NCMEC and when the matter is subsequently referred to law enforcement and a preservation request is issued.

Second, Yahoo! agrees that other ISPs should follow US ISPA's Sound Practices for reporting to NCMEC. When the reporting statute was passed, the Department of Justice was given authority to issue regulations pertaining to NCMEC reporting. The Department of Justice has not yet issued regulations on this subject. To fill this gap, the ISPs who are members of US ISPA worked with NCMEC to develop the sound reporting practices which Yahoo! and other major ISPs follow. Many other ISPs do not follow these practices, creating gaps in the protective net. Having worked closely with NCMEC, we know that if other ISPs followed these

practices, law enforcement would be in a better position to pursue all of the cases referred to NCMEC, not just the cases from a select few providers.

#### CONCLUSION

The Internet offers extraordinarily rich and diverse opportunities for children all over the world – to learn, to play, to explore and to discover. Internet connectivity helps level the playing field for many children, removing disadvantages resulting from poverty, isolation or disability. Yahoo! takes great pride in knowing that its efforts, programs and services bring hope and opportunity to so many youth across our nation.

Of course, just as there are challenges in the off-line world, the Internet presents challenges and threats of its own, reflecting the diverse and inconsistent motivations of the people who use it. Through the activities described in this testimony, Yahoo! has tried to make the Internet a safer place for children. While there will always be people who commit crimes online, just as there are those who do so in the real world, Yahoo! hopes that its actions make it less likely that people can abuse this vital medium to harm children, and that if they do, they will be identified, investigated and punished.

I look forward to working with the Members of this subcommittee to protect children in the online world. Thank you for the opportunity to testify today.

MR. WHITFIELD. Thank you, Ms. Banker. We appreciate the announcements made today by AOL, Yahoo!, Microsoft, EarthLink, and United Online Technologies in their new initiative.

Mr. Dailey, you are recognized for 5 minutes.

MR. DAILEY. Thank you very much, Mr. Chairman and Ranking Member Stupak and to members of the subcommittee.

Good afternoon. My name is Tom Dailey, and I am the General Counsel of Verizon Online, which is Verizon's consumer and small and medium Internet business offering DSL and other broadband services, fiber services, and so forth. I am also the former chairman of the U.S. Internet Service Provider Association. I was the chairman for approximately 4 years, and I am now the chairman emeritus of that organization. And I have been the General Counsel at Verizon Online for the past 8 years.

Like many in this room, I, too, am a parent. I have got two sons, each of whom, like many kids, is active on the Internet. I am as shocked as everyone by what I have seen this morning and other stories that I have seen and heard about as well as the work that we do from day to day in dealing with the types of people that we have been referring to as child predators. But they are really, often times, just common criminals, and we need more work. There is no question about it. And I agree with many of the comments that I have heard this morning from my colleagues and before.

Verizon shares the concerns that I think we all have. We are in a somewhat different place from Yahoo! and AOL, because we are a network service provider fundamentally. The services that we offer to our customers are primarily the Internet access component, the network component. When it comes to the services, the portal services, we have two very strong partnerships, one with Yahoo! and one with Microsoft, and they provide terrific services to our customers. We are primarily focused on the network access piece. We don't provide our own search. We don't provide our own chat rooms, so we are in a somewhat different position, as I indicated.

But Verizon has been a leader for many years in the area of online education, both in terms of the safety and security information that we provide to our customer, but also in terms of the Internet software and security software and parental control software that we make available both through our partners like Yahoo! and Microsoft but also through other services that we make available to our customers.

Verizon is also a proud participant in various cyber citizenship initiatives, including: GetNetwise, which is a campaign and website designed to give Internet users an online resource for information on Internet security; our participation with ICRA, the Internet Content Rating Association, is something that we value greatly; that association attempts to raise the level of awareness about content and threats online. Finally, our collaboration with i-SAFE America, which is creating a powerful set of cyber citizenship tools to educate K-12 students about responsible online behavior.



But Verizon does much more than simply provide online education resources, which we believe are, indeed, very important. We also are a very active participant in the investigation of online and real-world criminal activity involving crimes against children. We have a manual to help law enforcement to inform them about the types of services, the work and content and materials that we can provide to them and how they can come to us for help. And we provide a lot of help to law enforcement across the country at the State, local, and Federal levels.

Verizon has been active in a number of very important cases recently, and I mentioned several of them in my testimony. One I want to just highlight for you today, and that is the case in which Verizon provided key information to law enforcement that enabled the rescue of a 13-year-old Pennsylvania girl who had been abducted and held by a 39-year-old man as his sex slave. Through Verizon's help, law enforcement was able to locate and free the child who was found chained to a bed, otherwise relatively unharmed. And the individual that committed that crime is now serving a 20-year prison sentence. But it was Verizon's security group, Verizon's ability to find that user that helped, I think, save that girl's life.

I am not going to repeat all of the cases cited in my testimony, cases in which Verizon helped find runaways, in which Verizon helped prevent a child molestation, but we are proud of our role in assisting law enforcement to help in the area of child protection.

Verizon has been a participant, as have other members of the panel, with the National Center for Missing and Exploited Children's online CyberTipline program. We have done that for many years. Historically, because of our role as a network provider, we haven't seen as much of the child predation, very little, in fact, as some of the other companies before you. We have typically seen images. We report those images when we get those. But the bad guys, as I think Mr. Ryan indicated, are changing their modus operandi, and we recently observed what appears to be online child pornography spam as a result of that. We have adjusted our reporting to NCMEC, which is why, if you have looked at the data, we have had a spike in our reports from very few to actually over 100 this year, which is a significant increase from previous years. But the reason is that we are not just reporting images. We are now seeing a change. And so we have adapted, and we are reporting these apparent e-mail solicitations as well.

Verizon supports the initiatives that have been described previously about enhancing the ability of NCMEC to facilitate investigations of child pornography through the granting of authority to NCMEC to issue preservation orders. We believe that will be helpful. It will help preserve data and make it available for law enforcement later on. And

we support changes in the reporting statute under 13-032 to make it clear that ISPs that report to NCMEC can include images of child pornography with their electronic submissions without the risk of that being deemed a distribution of child pornography. We think that these changes will enhance reporting and improve law enforcement's ability to investigate and prosecute those who prey on children.

I look forward to your questions, and thank you again for this opportunity to participate.

[The prepared statement of Tom Dailey follows:]

PREPARED STATEMENT OF TOM DAILEY GENERAL COUNSEL, VERIZON COMMUNICATIONS

Mr. Dailey's testimony focuses on Verizon's efforts to fight online child exploitation through cooperation with law enforcement, the delivery of online tools and educational programs to Verizon Online subscribers, and cyber-citizenship initiatives targeted to all Internet users. With respect to Verizon's retail Internet access services, the testimony describes the differences between Verizon Online's role as a network provider and its use of third party portals to provide chat, forums and other online services and how this business arrangement affects reporting of child pornography incidents. The testimony further describes several instances in which Verizon, through collaboration with law enforcement and other ISPs, has successfully assisted in the rescuing of children (and the prevention of possible child molestation). Mr. Dailey's testimony also describes how Verizon reports potential instances of child pornography under 42 USC §13032. The testimony concludes with the proposal of two statutory changes which Verizon believes can be fairly simply accomplished and which will significantly enhance the effectiveness of law enforcement efforts to track down and prosecute child exploitation crimes.

# **I. Introduction**

Chairman Whitfield, Ranking Member Stupak members of the subcommittee, thank you for the opportunity to testify here today. The people of Verizon believe that the issue of online child safety is very important and Congress can help by making some improvements in the current laws. At Verizon there is a very strong belief in our responsibility as a corporate leader to do what is right. We believe helping to protect children from online predators, and assisting law enforcement in their efforts to track down those who would exploit children through the Internet, is the right thing to do. We are a part of a quickly transforming industry moving from the old world of basic telephone service to a new world of broadband networks. Not long ago people communicated through telephone calls and the Internet was something that only a techie could understand how to use. We are now in a very different era where people connect with one another around the globe in an instant and transmit and receive images via the Internet with the click of a mouse. As remarkably beneficial and enriching as the Internet has become, there comes with this technology a darker side that includes new ways to carry out old criminal activity. Child exploitation is one example. Verizon takes the issue of fighting child exploitation very seriously and we are here today with the goal of finding new ways to combat the spread of child pornography. We applaud the efforts of this Committee, of those at the National Center for Missing and Exploited Children, and of others in the law enforcement and ISP communities, who are dedicated to the fight against child exploitation. In this spirit, Verizon offers the following testimony.

## **II. Verizon as a Network Provider and its Online Safety and Security Services**

a. Verizon's Internet Access Services Operations. Verizon is a wholesale and retail provider of communications, data and video services to a wide array of customers ranging from individual consumers to multi-national corporations. In the data world, Verizon provides two primary wireline Internet access technologies: (1) dial-up Internet access service that is provided primarily on a wholesale basis to large, consumer-focused Internet service providers; and (2) high-speed Internet access service, that is provided to retail consumer and business users. Verizon's high-speed services for consumers use digital subscriber loop ("DSL") and fiber-based (commercially known as "FiOS") technologies. Both services provide high-speed Internet access and transmission capabilities. The Verizon business units that offer Internet access services include Verizon Online, which is retail focused and currently has more than five million consumer and small/medium sized business subscribers nationally; and Verizon Business, which sells a variety of wholesale and retail Internet access services to thousands of enterprise (large) businesses and government entities.

The structure of Verizon Online's consumer Internet service differs from many in the industry. All subscribers to the company's retail consumer Internet access service, whether DSL- or fiber-based, receive a choice of portal providers when they register for their broadband service. Subscribers can choose to receive as part of their Internet access package co-branded premium portal services from Yahoo! or MSN. The services they receive from these companies are specially designed to combine certain Verizon-provided features (such as account management tools and email) with the portal provider's own content, features and functionality (such as instant messaging, email, chat, search, entertainment and other online services). This unique blending of Internet access with portal features and services has an impact on the volume of child pornography reports Verizon refers to NCMEC, which I'll discuss further in my testimony, below.

b. Verizon Online's Safety and Security Offerings. Verizon Online makes available to its subscribers a variety of Internet security services provided by Yahoo! and MSN. Each portal provides anti-virus, firewall, anti-spyware and parental control software, which currently are provided at no extra charge to Verizon Online subscribers. In addition to making the Yahoo! and MSN security services available to its subscribers, Verizon Online offers its own, private-labeled suite of security services. This security suite includes anti-virus, firewall, anti-spyware and parental control software and is available for an additional monthly charge. Historically, Verizon Online has also made commercially available parental control software offered by CyberPatrol and Cybersitter to its subscribers at a discount off the normal retail price.

In addition to its history of providing subscribers with the tools they need to help protect themselves and their children from harmful viruses and objectionable content, Verizon Online has also worked to help educate its subscribers about Internet threats of all kinds. The company's Safety and Security website, one of the first of its kind among network providers, gives our customers access to Internet sites designed to help parents learn about ways to protect their children online, including links to the National Center for Missing and Exploited Children's ("NCMEC") website and CyberTipline for reporting incidents of child exploitation or pornography, GetNetWise (a site dedicated to educating about dangers on the Internet), StaySafeOnline and OnGuard Online (an education site offering advice regarding the safe use of chat and community networking services). Verizon Online has participated in national events such as National CyberAwareness month, which it publicized to its subscribers, and the company periodically distributes helpful information through its newsletters on wide-ranging topics that include cyber-safety.

c. Differences Between Verizon's Internet Access Services and Other Online Services. Unlike AOL, MSN and Yahoo!, Verizon Online does not currently provide

chat rooms, online forums or blog sites. Although Verizon Online has provided web hosting services targeted to business users, and storage services for all users, these services to this point have not been particularly widely adopted. Thus, because Verizon Online is primarily a network access services company, and because the vast majority of its subscribers use one of the portal services provided by its portal partners, Verizon Online sees very few complaints involving actual images of child pornography and virtually no complaints of predatory activity. It is Verizon Online's belief that complaints regarding child pornography and predation activity primarily go to the providers of the forums in which the illicit activity takes place, e.g., chat rooms and community network sites. The few reports of actual child pornography Verizon Online has historically seen have related more to content residing on its web hosting service. The vast majority of reported child pornography incidents that Verizon Online *now* receives have been in the form of emails (largely spam-related) that the company's subscribers forward to Verizon Online's security abuse email box.

### **III. Cooperation with Law Enforcement, Case Studies and Cyber-Citizenship**

Verizon has a long history of working cooperatively with law enforcement in the investigation of criminal activity, including fighting child pornography. Through these efforts Verizon has played an important role, among other things, in securing the safe return of missing children and even in saving lives. Outside the security context, Verizon has played a prominent role in the development of cyber-citizen initiatives, online safety programs and customer education websites designed to promote the public safety at large.

a. Cooperation with Law Enforcement. Verizon as a corporation handles thousands of law enforcement subpoenas every month through its voice and data communications security organizations. In the Internet context, Verizon Online processes more than 100 criminal subpoenas a month (706 so far in 2006). The Verizon Online and Verizon Business security group work with local, state and federal law enforcement officials to investigate claims ranging from property crimes (fraud, phishing and identity theft) to threatened physical harm to child pornography. Verizon Online and Verizon Business each have dedicated personnel who work with law enforcement to respond to legal process (subpoenas, court orders and warrants) and to help law enforcement in their efforts to identify the information they need to track down illegal activity on the Internet.

Verizon Online's security group has worked diligently and cooperatively with law enforcement across the country, and with other ISPs, on investigations ranging from post 9/11 watch-list cases to tsunami fraud schemes to tracking child predators and missing children. In one highly publicized case in 2002, Verizon Online played a critical role in tracking down and saving the life of a 13 year old Pittsburgh girl who had been abducted by a 38 year old Herndon, Virginia man named Scott Tyree. After abducting the girl, Tyree was observed in a Yahoo! chat room apparently bragging about what he had done. A participant in the chat room linked Tyree's forum discussion to stories heard on the news and reported the incident. Law enforcement tracked Tyree through Yahoo! and ultimately determined that his Internet connection showed to a Verizon IP address, meaning he likely was a Verizon Online subscriber. Working with the FBI, Verizon Online's security team was able to determine the exact location of the computer Tyree was using and provided this information to law enforcement. A waiting SWAT team then raided Tyree's Herndon condominium to find the victim tied to a bedpost but relatively unharmed. Tyree is now serving a nearly 20 year prison sentence.

The Tyree case is but one example of the successes that cooperation between Verizon security and law enforcement personnel has brought in child exploitation and endangerment cases. Verizon Online security has worked with noted Polk County Sheriff's Department investigator Charlie Gates on child predation related cases and with local law enforcement personnel across the nation. Verizon Online has also worked

closely with its ISP colleagues to locate missing children. In one case, Verizon Online and AOL teamed up to track down a runaway who was logging into her AOL instant messenger account from Internet cafés across several states. As the child logged into her AIM account, AOL and Verizon Online security personnel tracked the child's location based on the location of the Internet connection and ultimately to were able to help facilitate the child's safe return. In yet another case, the quick action of a Verizon Business security team member in processing a subpoena helped police prevent the molestation of a minor.

Finally, in a child kidnapping case, Verizon security personnel received notice from a Bridgewater, New Jersey, detective that a 5 month old child had been kidnapped from a babysitter. Verizon security performed record searches and was able to discover a series of cellular and voice over IP calls that seemed like a promising lead. Verizon's investigator then coordinated with Verizon Wireless and Sprint regarding the cellular calls and with Level 3 Communications regarding the voice over IP calls, all after hours, to set up emergency assistance for the investigating detective. The next day, the detective handling the case called to inform Verizon security that the voice over IP investigation had helped lead them to the kidnapped infant and that the child was safe. These stories are but a few examples of the things Verizon security personnel do day in and day out to help law enforcement to do its job.

b. Cyber-Citizenship Initiatives. Verizon has long been a major player in advancing cyber-citizenship principles and promoting online safety for children and all Internet users. As noted above, Verizon was one of the first major ISPs to develop an online safety and security website that offers Verizon Online subscribers a variety of information and tools to help protect against Internet threats and parents to help safeguard their children online. Verizon was one of the founders of GetNetWise.org, a campaign and web site designed to give Internet users an easy, online resource for additional information on Internet security, include ("ICRA") to deliver an education campaign to raise the level of awareness about content threats in our converged world. Verizon and ICRA are working cooperatively to answer parents' questions and point them to the tools they can employ to help protect their children from harmful online content. Finally, Verizon is collaborating with i-SAFE America, Inc. on a multi-year initiative to create a powerful set of cyber-citizenship tools that educate K-12 students about responsible access to entertainment, information and online communication tools, including issues related to social networking sites, chat rooms, and online bullying.

Verizon has also participated with NCMEC and the US Internet Service Provider Association ("USISPA") in crafting a series of industry best practices regarding the reporting of child pornography, and in finding ways to enlist the support of and to educate smaller ISPs about child pornography enforcement and reporting. The company is currently working with the Department of Justice and its task force on child pornography enforcement to look at ways in which the ISP industry can work with law enforcement to improve child pornography enforcement, whether through data preservation or retention or other means. In short, Verizon has been a prominent participant in the discussion on child pornography enforcement, and in outreach efforts involving its own customers and Internet users at large. Through these efforts, and its ongoing work with law enforcement, Verizon has demonstrated its firm commitment to helping safeguard children on the Internet and to assisting law enforcement in pursuing those who would use the Internet to exploit children.

#### **IV. Child Pornography Reporting**

Although Verizon Online does not receive the volume of child pornography related cases as other ISPs do, the company maintains a full-time security analyst who monitors Verizon Online's abuse mail box for child pornography complaints and reports. (Virtually all reports of child pornography come to Verizon Online through its abuse

email boxes). Once identified as a reportable incident under 42 USC §13032, Verizon uses the NCMEC ISP Tipline to report the incident to NCMEC. Verizon is a registered user of NCMEC's ISP CyberTipline.

While Verizon Online has always reported incidents of child pornography to law enforcement, over time its approach to assessing what is and is not a reportable incident under 42 USC §13032 has changed. Historically, Verizon Online focused its reporting on instances of child pornography images found to be housed on Verizon Online servers. Because of its role as a network provider, with no chat or forum services of its own and only a small web hosting business, the volume of reportable child pornography incidents Verizon Online has received and made has been quite small (roughly 12 over the past 6 years). We attribute this small number of cases to the fact that the circumstances under which Verizon Online subscribers most often encounter child pornography involve the use of services not provided by Verizon Online today (IM, blogging or chat/forum services), or involve websites not hosted by Verizon Online. If an Internet user encounters child pornography when visiting a third-party site, they are most likely in our experience to report the incident to the third-party, not Verizon.

Recently, Verizon Online changed its reporting criteria to broaden the categories of child pornography complaints that it passes on to NCMEC. Verizon Online observed that the vast majority of child pornography complaints it was receiving pertained to email solicitations (often spam) relating to child pornography. In analyzing these complaints, Verizon Online concluded that the emails themselves could be viewed as facts or circumstances from which a violation of the child pornography laws was apparent under 42 USC §13032. As a result, Verizon began reporting these email complaints to NCMEC in April 2006.<sup>1</sup> Since that time, Verizon Online has filed 116 reports using the CyberTipline, the vast majority of which were in the form of emails forwarded by customers, which Verizon Online in turn forwarded on to NCMEC via the CyberTipline. The balance was child pornography related emails actually received in Verizon's own email boxes. Many of these emails contain URLs that purportedly link to content containing child pornography. None of the 116 customer complaints contained actual images of child pornography.

## **V. Legislative Improvements to Child Pornography Enforcement**

Verizon supports improvements to current laws regarding child pornography enforcement, rather than the creation of new mandates. In particular, we see two areas in which Congress can make significant improvements in the enforcement effort, without engaging in a wholesale re-write of existing law. First, Congress should authorize NCMEC to issue preservation requests under 18 USC §2703(f). NCMEC is not a governmental entity, yet it has been charged with the responsibility to coordinate the investigation of child pornography and related cases by law enforcement. Securing the availability of electronic data is an important element to such investigations; empowering NCMEC to request preservation immediately upon receipt of a colorable report of child pornography makes sense and would significantly expedite the process of securing potentially relevant information.

Second, Congress should clarify under 18 USC §2252A that submission by an ISP of images of child pornography as part of a bona fide report under 42 USC §13032 does not constitute the unlawful distribution of child pornography. The current statutory

---

<sup>1</sup> There was a process delay in early 2006 that interrupted Verizon Online's reporting early in the year as the company reorganized its abuse group and the reporting responsibility transitioned to a new staff member. At this time Verizon Online security also experienced network connectivity problems and delays in re-establishing its ISP Tipline account that contributed to the interruption in reporting. The connectivity issue was remedied and Verizon Online resumed reporting in April 2006.

scheme is ambiguous on this issue and the ambiguity should be eliminated. Clarification that the submission of images as part of a report to NCMEC or law enforcement is not unlawful distribution of child pornography will encourage more ISPs to report images, and thereby facilitate investigations into the reported image. Verizon urges this Committee to clarify this point.

Finally, there has been much discussion of late on the issue of data retention in the context of child pornography investigations. The expressed position of law enforcement is that data retention may be necessary to ensure that the data necessary to enable investigators to identify the user of an IP address assigned to a particular user's Internet session is present when requested. The reason IP address assignments are useful to law enforcement is because an IP address is often an important link between illicit conduct on the Internet and the identity of the alleged perpetrator. While the debate over data retention is still forming, Verizon's general view is that IP address assignment and customer record information collected in the normal course of business could be retained by network providers for a reasonable period of time, and if retention is required, that the period of retention should be long enough reasonably to enable law enforcement to conduct their investigations. Whether this obligation should extend to others in the Internet community is still open to debate, as is whether the period of retention should be 24 months (as has been proposed) or a shorter period more in line with the retention policies of businesses in effect today.

There are two important caveats to this position, however. First, any such data retention requirements should apply only to IP address assignment information, and it should apply only to data gathered in the normal course of business. Verizon Online believes that many network providers already capture helpful information in connection with their standard processes for providing and/or billing for services. A retention requirement for IP address assignment data currently gathered in the normal course of business may be a reasonable first step that balances the needs of law enforcement with the national desire to keep the Internet free from extensive regulation and regulation-related costs. Second, the availability of data retention should not preclude granting NCMEC the data preservation authority discussed above. Data preservation will go a long way toward protecting data that might otherwise be deleted over the passage of time between the date an incident of child pornography is reported to NCMEC and the issuance of a subpoena or other legal process by a downstream law enforcement official. An order to preserve data will not guarantee that data will be present when requested, but it will greatly improve the chances that data which is captured will be available to law enforcement at the time it is subpoenaed.

Thank you for this opportunity to present Verizon's views on this important issue.

MR. WHITFIELD. Thank you, Mr. Dailey.

And Mr. Lewis, you are recognized for 5 minutes.

MR. LEWIS. Thank you, Mr. Chairman.

Mr. Chairman, Ranking Member Stupak, and members of the subcommittee, I appreciate the opportunity to testify before you today on behalf of Comcast regarding the important subject of making the Internet safe for kids.

My name is Jerry Lewis. I am the Vice President, Deputy General Counsel, and the Chief Privacy Officer of Comcast.

Comcast is America's leading provider of high-speed Internet services with over 9 million customers. And the safety and security of

our customers, along with the quality of our service, are very important concerns.

We are committed to leadership in the area of online security and customer privacy and in cooperating with law enforcement to fight Internet-based criminal activity, such as child exploitation. At no extra cost to our customers, we provided a filtered Internet search option and easy-to-use privacy and parental control software that lets parents monitor chat and online activity, block inappropriate content, and prevent their children from sharing personal information.

We have a solid record in assisting law enforcement, and we have received numerous commendations for our efforts. We distribute a guide to law enforcement regarding how to obtain prompt handling of their requests. We conduct training for law enforcement, and we meet quarterly with DOJ and FBI law enforcement officials to discuss ways that we can work together quickly and smoothly nationwide.

But neither we nor any other Internet service provide, or ISP, is perfect. During a massive build-out phase of our Internet protocol, or IP, network last year, we had significant difficulties in meeting many law enforcement requests due to problems with our network's customer provisioning system. Thankfully, that phase is behind us, and we are committed to best practices in this area.

Because of the importance of child safety, we want to do more. We have decided to extend our retention of IP address assignment information to 180 days. We are making the investment necessary to implement this change by September 1. We understand that our current IP address retention period is shorter than many other large commercial broadband ISPs. We established our IP address retention period at a time when Federal and State officials raised privacy concerns about retention of other data on our systems, so we erred on the side of setting a shorter time period. Comcast will voluntarily take this significant step to accommodate more valid law enforcement requests in a manner that is consistent with the privacy expectations of our subscribers and the law.

To be very clear, however, we will only retain IP address assignment information, information that we already retain for 180 days and will retain no additional information, unless compelled to do so by valid legal process. We are committed to striking the delicate balance between customer privacy and being able to provide evidence in response to investigations of online crimes.

Based upon our experience, we believe that the following other measures would contribute significantly to improving child safety online and hope the subcommittee will recommend them. First, greater public and private-sector efforts to educate families about the dangers of online pedophiles and the importance of parental involvement and technology



to protect children, and I believe Chris Hansen's presentation earlier in the day underscores that fact. Second, greater resources for law enforcement teams combined with increased training and forensic support in the private sector so that law enforcement can trace hard-to-find perpetrators. Third, is giving the National Center for Missing and Exploited Children, or NCMEC, subpoena power so that it can gather critical evidence relating to reports that it receives without the delay of waiting for a referral to Federal or State law enforcement. Fourth, preservation of evidence known by an ISP to be relevant to a NCMEC report as a matter of course without waiting for a preservation order so that the evidence will be available for law enforcement. Finally, where available, is submitting relevant IP address assignment information and town and State information in reports to NCMEC to facilitate referrals to the proper law enforcement authorities.

In closing, Comcast is committed to a safe and secure Internet and to working with the Attorney General, this subcommittee, and everyone in the ISP industry to craft the right policies that balance the needs of law enforcement with customer privacy expectations. Child exploitation is a heinous crime. We intend to assume a leadership role in the solution to combating it.

Thank you, and I look forward to answering your questions.

[The prepared statement of Gerard J. Lewis, Jr. follows:]

PREPARED STATEMENT OF GERALD J. LEWIS, JR., VICE PRESIDENT, DEPUTY GENERAL  
COUNSEL & CHIEF PRIVACY OFFICER, COMCAST CABLE COMMUNICATIONS

**Summary of the Testimony of Gerard Lewis**

Comcast is America's leading provider of high-speed Internet services with over nine million customers. And the safety and security of our customers, along with the quality of our service, are our foremost concerns. We are committed to leadership in the area of online security and customer privacy, and in cooperating with law enforcement to fight Internet-based criminal activity such as child pornography. At no extra cost to our customers, we provide a filtered Internet search option and easy-to-use privacy and parental control software that lets parents monitor chat and online activity, block inappropriate content, and prevent their children from sharing personal information.

We have a solid record in assisting law enforcement, and we have received numerous commendations for our efforts. We distribute a guide to law enforcement regarding how to obtain prompt handling of their requests, we conduct training for law enforcement, and we meet quarterly with DOJ and FBI law enforcement officials to discuss ways that we can work together quickly and smoothly nationwide. But neither we nor any other Internet service provider (or ISP) is perfect. During a massive build-out phase of our Internet protocol (or IP) network last year, we had significant difficulties in meeting many law enforcement requests due to problems with our network's customer provisioning system. That phase is behind us, and we are committed to best practices in this area.

Because of the importance of child safety, we want to do more. We understand that our IP address retention period is shorter than that of many other large commercial ISPs. We established our IP address retention period at a time when federal and state officials raised privacy concerns about retention of other data on our systems, so we erred on the side of setting a shorter IP address retention period. Comcast will voluntarily take a significant step to accommodate more valid law enforcement requests in a manner that is consistent with the privacy expectations of our subscribers and the law. We have decided to retain IP address assignment information for 180 days. We are making the investment necessary to implement this policy by September first.

To be very clear, we will *only* retain IP address assignment information – information that we already retain - for 180 days and will retain no additional information unless compelled to do so by valid legal process. We are committed to striking a delicate balance between customer privacy and being able to provide evidence in response to investigations of online crimes.

Based upon our experience, we believe that the following other measures would contribute significantly to improving child safety online and hope the Subcommittee will recommend them:

- Greater public and private sector efforts to educate families about the dangers of online pedophiles and the importance of parental involvement and technology to protect children;
- Greater resources for law enforcement teams combined with increased training and forensic support from the private sector so that law enforcement can trace hard-to-find perpetrators;

- Giving the National Center for Missing and Exploited Children (or NCMEC) subpoena power so that it can gather critical evidence relating to reports that it receives without the delay of waiting for referral to federal or state law enforcement;
- Preservation of evidence known by an ISP to be relevant to a NCMEC report as a matter of course without waiting for a preservation order so that the evidence will be available for law enforcement; and
- Where available, submitting relevant IP address assignment information and town and state information in reports to NCMEC to facilitate referrals to the proper law enforcement authorities.

Comcast is committed to a safe and secure Internet, and to working with the Attorney General, this subcommittee and everyone in the ISP industry to craft the right policies that balance the many countervailing concerns with which we must deal. Child pornography is a heinous crime. We intend to assume a leadership role in the solution to combating it.

Mr. Chairman, Ranking Member Stupak, and members of the Subcommittee:

I appreciate the opportunity to testify before you today on behalf of Comcast regarding the important subject of making the Internet safe for kids. My name is Jerry Lewis and I am a Vice President, Deputy General Counsel and Chief Privacy Officer of Comcast. My responsibilities include overseeing Comcast's national security and law enforcement compliance and privacy efforts. I am deeply involved in Comcast's extensive efforts to make the Internet a safe place for all our customers.

I commend the Subcommittee for its interest in and hard work on this important issue. Protecting children online is a critical responsibility in the online world and requires thoughtful and creative responses from government, non-profits and businesses alike.

### **1. How Comcast Protects Kids Online**

Protecting the safety of children online is one of our highest priorities. Comcast is committed to providing parents with effective tools and educational materials so that they can shield their children from offensive and inappropriate content on the Internet. Since we initiated our high-speed Internet service, Comcast has worked actively with a number of leading online safety organizations to follow and refine best practices in this area.

The SafeSearch feature of our online search gives parents the ability to filter children's Internet searches to exclude sexual-themed sites. Comcast also provides all of our customers with firewall, security, and privacy and parental control software from McAfee, a leading vendor, at no additional charge. All new customers receive information about this easy to download, valuable software from the prominently featured "Security Channel" on our portal, Comcast.net.<sup>1</sup> McAfee is simple to use and employs enhanced content filtering techniques to give parents the power to prevent the display of unwanted and offensive Internet content. A filtering option within the privacy service enables parents to monitor chat and other activity, block inappropriate or offensive content, and prevent the sharing of personal information by their children. An event-logging feature that parents may activate chronicles lists of websites visited, websites blocked, and inappropriate chat sessions.

Comcast's "Security Channel" encourages parents to be involved in their children's online surfing experience and provides additional information not only on the McAfee service, but also hyperlinks to educational websites such as [www.staysafe.org](http://www.staysafe.org), which provide more information about child safety online. Our site also addresses various technical issues that can

---

<sup>1</sup> See <http://www.comcast.net/security/mcafee/#parental>; attached as "Appendix 1".

compromise security – for example, we caution our customers to secure their home wireless connections so that they cannot be used by others.<sup>2</sup>

While many of the companies on today's panel function as Internet service providers ("ISPs") and each of us plays a role as a source of evidence for law enforcement investigations, it is important to understand how our businesses differ. Unlike many of the other ISPs, Comcast does not provide extensive features or services that permit our customers to post their own content for others to see and share or to interact in real time with others. As you know, places such as online chat rooms, groups, or forums where children meet adults present some of the most serious risks. We do not provide such services for general use by our customers.

## **2. Comcast's Work With Law Enforcement and Protection of Customer Privacy**

Comcast works closely with law enforcement agencies to provide timely and accurate responses to their requests, and we believe that we have solid overall working relationships with those agencies. Comcast has a Legal Response team dedicated to responding to requests from law enforcement for Comcast High-Speed Internet information, and I am the lawyer who works most closely with that group. Currently, we are usually able to process and respond to law enforcement requests for information within seven business days. In true emergency situations we can usually respond to law enforcement requests in hours, and sometimes minutes. When we learn of likely incidents of child pornography or child exploitation on our network, we report these activities directly to the National Center for Missing & Exploited Children (NCMEC).

In order to cooperate effectively with law enforcement agencies, we must educate these agencies about the type of evidence they can obtain from us and how to obtain it. This past spring, we published a comprehensive Law Enforcement Guide which is distributed through

<sup>2</sup> See <http://www.comcast.net/help/faq/index.jsp?faq=Security118072>; attached as "Appendix 2"

numerous law enforcement online bulletin boards. The Guide gives law enforcement personnel the help they need to ensure that requests to Comcast are handled and processed as quickly as possible. In addition, our National Security Operations team and I meet for several hours several times each year with Department of Justice and FBI law enforcement officials based in Philadelphia and in New Jersey to exchange current information regarding cyber-crime, to obtain feedback on our law enforcement response efforts, and jointly to figure out better ways for us to work quickly and smoothly together. We are continually working to improve best practices to ensure that law enforcement receives necessary information after submitting lawful evidentiary requests. Our team is available to, and has provided, formal and informal training to law enforcement officials and I have personally provided training to law enforcement agents.

Law enforcement agents have praised our response to their requests. In the past month alone, for example, we received several letters from law enforcement officials describing the responsiveness of our Legal Response team in child abuse and child pornography investigations as “outstanding,” and its efforts as “herculean.”<sup>3</sup> They credit our Legal Response team for having “immeasurably assisted” child pornography and exploitation investigations and for having “impacted the worlds of so many and made this world a better place.” In our most recent quarterly meeting, law enforcement officials specifically praised the speed of our processing of legal requests, and our care to produce accurate responses. While we are very proud of this feedback, neither we nor any other ISP is perfect. During a massive build-out phase of our Internet protocol (“IP”) network last year, we had significant difficulties in meeting many law enforcement requests due to problems with our customer provisioning system. That phase is behind us, and we are committed to best practices in this area.

---

<sup>3</sup> The law enforcement letters appear at the end of this testimony; attached as “Appendix 3.”

We continue to seek ways to provide top-notch service in response to lawful law enforcement requests, and we also continue to expand our Internet law enforcement compliance team as our business grows.

Comcast is proud of its record assisting law enforcement when they present us with valid legal requests. But our customers should understand that we are strongly protective of their privacy and we are proud of our efforts here, too. Comcast strictly limits the kind of information it collects and retains about its Internet customers. We are extremely mindful of customer privacy, and it has been our policy and practice to collect and retain only information necessary for service delivery and network operations and management. We store this limited information for only as long as necessary for the purpose for which it was collected. We don't track or retain web page visits of our Internet customers on a personally identifiable basis, unless compelled to do so by valid legal process such as a court order, for example.

We must walk a fine line between preserving the privacy of our customers and meeting the legitimate needs of law enforcement. As a cable company, we are governed by the very strict privacy provisions of Section 631 of the Cable Act, found at 47 U.S.C. Sec. 551, and we comply with this law for our Internet service. Moreover, we were further deeply sensitized to the importance of our privacy obligations when, in early 2002, it was reported that Comcast might be caching certain web usage information on a non-personally identifiable basis— with no intention of having it identifiable to any particular customer — in order to facilitate network management. The public reaction was strong and swift, from a Member of Congress and three state attorneys general, among others. While we neither did nor intended anything wrong or in violation of the law, we acted within 48 hours of contact to cease that information collection in order to assure our customers of our privacy commitment to them. At that time, we decided to



retain IP address assignment data<sup>4</sup> for the absolute minimum amount of time necessary for network management – 31 days.

We remain sensitive to striking the appropriate balance between customer privacy and law enforcement interests. We understand that our 31-day IP address retention policies places us at the low end of typical broadband industry practices. We recognize the increasing importance that this type of information plays in advancing child pornography and child exploitation investigations. Therefore, in an effort to strike the appropriate balance between accommodating valid law enforcement requests and protecting the privacy expectations of our subscribers, we have decided to implement a 180-day retention policy for this IP address assignment data. One of the reasons for this change is to provide increased support for child exploitation investigations. We are working to make sure that this new policy will take effect by September 1. We are confident that this policy will enable Comcast to become more responsive to valid law enforcement requests for IP address information.

I stress that the kind of data that we routinely retain, and that law enforcement agencies routinely request from us, is strictly limited. That data consists of IP address assignments – the “temporary number” that we assign to a personal computer connected to our network – which we are able to match up to other information provided to us by law enforcement in order to identify a suspected lawbreaker. We do not retain information on any customer’s Internet use or web-surfing habits. We will only retain such information when a law enforcement agency obtains a court order as required by law.

---

<sup>4</sup> When a PC or other device connects with our Comcast High-Speed Internet service, it is assigned a temporary IP address. This “dynamic IP addressing” means that a customer’s PC will be assigned different IP addresses by our service over time. Dynamic IP addressing helps us to manage our network more efficiently and add new customers quickly and seamlessly.

We are committed to be a leader among ISPs in striking the right balance of interests. We were part of the first small group of ISPs to meet with the Attorney General and the director of the Federal Bureau of Investigation to initiate a dialogue on ways to make child pornography and child exploitation investigations more effective. A key topic of discussion has been the development of uniform industry policies on the length of time that ISPs should retain records of which IP address was assigned to which connected personal computer at which time. We appreciate the opportunity to be a part of this important dialogue.

### **3. How to Improve Child Safety Online**

As the Subcommittee's hearings have made abundantly clear, both government and the private sector can and need to do more to attack the problem of online child exploitation and child pornography.

Based upon our experience, we believe that the following initiatives would contribute significantly to improving child safety online, and we hope that the Subcommittee will recommend them.

#### **a. Improved Education of Parents and Children.**

The best way to thwart child exploitation is to educate parents and children about the dangers posed by pedophiles, the importance of parental involvement in a child's Internet activities, and technology tools that help to protect children from pedophiles. Specific warnings in chatrooms, for example, can educate children who are at greatest risk. Public education is an area where the private sector has and should continue to take the lead, although government involvement is, of course, most welcome.

**b. Increased Training and Technical Support for Law Enforcement Investigating Cybercrime.**

In our experience, there is no more valuable investment in pursuing online predators than in adequately staffing law enforcement teams, training law enforcement regarding effective investigative techniques, and providing law enforcement with sufficient technical support to trace hard-to-find perpetrators. This is a resource question. While government must take the lead, the private sector can and should help, particularly with regard to training and forensic assistance. We are prepared to work with others in the ISP industry to provide more training to law enforcement officials, as well as direct forensic assistance to law enforcement officials tracking hard-to-find child predators.

**c. Give NCMEC subpoena power**

Like most others in the ISP industry, Comcast submits reports of suspected child pornography to NCMEC. However, based on testimony previously delivered before this Subcommittee, we understand that a relatively small number of reports to NCMEC lead to a prosecution. A major focus of reforms should be to make these leads yield greater results.

NCMEC functions as a national clearinghouse for reports of online child pornography and child exploitation. However, NCMEC itself does not have subpoena power and must wait for federal or state law enforcement to follow up on these leads. If NCMEC itself had subpoena authority, it would have the option of gathering evidence without the delay involved in the referral process.

**d. Data preservation when entities make mandatory reports to NCMEC.**

To ensure that evidence is available when law enforcement follows up on reports to NCMEC, we recommend preservation, for a defined period, of available evidence in a service provider's possession that it knows to be relevant to the referral. "Data preservation" is the retention of evidence relevant to a particular investigation for a defined period so that it can be subpoenaed by law enforcement at a later date. A data preservation requirement upon a report to NCMEC would ensure that relevant, limited data would be available to law enforcement beyond the individual data retention periods observed by individual ISPs.

**e. Provision of IP address assignment data and locality information regarding the suspect in reports to NCMEC.**

When service providers have relevant IP address assignment information and town and state information relating to apparent child pornography, that information should be included in reports to NCMEC. We think that this extra level of detail—which many ISPs currently provide—would facilitate referrals to the right law enforcement officials and give agents a leg up in investigations where this information is available.

We are, of course, open to considering other ways to address this deeply troubling problem, but believe that these are effective means. The entire ISP community, and application and service providers as well, must continue to devise and implement new solutions to combat child pornography and exploitation.

**4. Conclusion**

Protecting child safety online is a critically important responsibility that Comcast takes very seriously. We appreciate the Subcommittee's holding this series of hearings on the subject, and hope that they prompt smart, effective initiatives by both government and the private sector that will make progress in the fight to keep children safe online.

## APPENDIX 1

[Mail](#)
[Radio](#)
[Photos](#)
[Video](#)
[Security](#)
[Sign In](#)
[Ask Comcast](#)

[Web](#)
[Images](#)
[Video](#)
[Shopping](#)
[Help](#)

Search the Web:   [More...](#)

[HOME](#) > [SECURITY](#)
[Go to Express](#)
[Help](#)
[My Account](#)

[HELP:](#) [Ask Comcast](#) | [FAQs](#) | [One Click Fixes](#) | [Desktop Doctor](#) | [Help Forums](#) | [Email Us](#) | [Live Chat](#)  
[SECURITY:](#) [Anti-Virus](#) | [Personal Firewall](#) | [Privacy Service](#) | [Anti-Spyware](#) | [Security Alerts](#) | [Security Forums](#)  
[MY ACCOUNT:](#) [Reset Password](#) | [Create Additional Email Account](#) | [Enable PWP](#) | [Pay Bill Online](#)

## Cut Down on Spam

Is spam taking over your inbox? Find out what you can do to cut down on bulk e-mails.

### PROTECT YOUR COMPUTER

Protect your computer with proven McAfee Security downloads included **at no additional cost** with your Comcast High-Speed Internet Service! [Learn more and download them today.](#)

**! Already registered for McAfee services?**  
To download, install or reinstall McAfee security tools, [click here.](#)

**Need help with McAfee Security Downloads?**  
Visit [Comcast's McAfee Help Site.](#)

**McAfee VirusScan**

to Defend your computer against thousands of known viruses. VirusScan is easy to use and install and will automatically check for updates and upgrades to help protect your computer from virus attacks. Offer not valid for Macintosh customers. [Learn more.](#)

**McAfee Personal Firewall Plus**

### SEARCH HELP

**ENTER SEARCH WORD**

### SECURITY ALERTS

**06-19-2006: COMCAST PHISHING ALERT**

**Issue Description:** Customer reported receiving an email directing customers to a site claiming to be from Comcast, that directed the subscriber to a Web page hosted in Turkey that may fraudulently request billing, credit card, and other personal information.

**Subject:** **Your account with Comcast.**

It has come to our attention that your Comcast Verification details records are expired. This requires that you update your Comcast Profile records immediately. Failure to update your records will turn out in account termination. Please update your records within 48 hours. Once you have updated your account records, your Comcast account will not be terminated and will continue as normal. Failure to update will result in Terms of Service violations, termination of service or future billing problems. Please click here to continue. (*url has been removed*)

**US CERT: MICROSOFT EXCEL VULNERABILITY**

**REGISTER NOW**

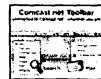
A firewall is an essential part of your high-speed Internet experience. Protect your personal information and your computer from malicious intruders. Offer not valid for Macintosh customers. [Learn more.](#)

**McAfee Privacy Service****REGISTER NOW**

McAfee Privacy Service features parental controls to help filter out inappropriate content and also monitors Internet activity to help prevent identity theft. Offer not valid for Macintosh customers. [Learn more.](#)

**Protect your PC with the Comcast Toolbar****DOWNLOAD NOW**

Easy-to-use Security features include:



**McAfee Security** - One-click access to McAfee VirusScan, Firewall, and Privacy Service

**Pop-up blocker** - Block pop-up ads that interfere with your Web surfing experience.

**Anti-spyware** - Easily detect and remove spyware from your PC that can slow down your PC's performance and track your Web activity without your knowledge.

Best of all, the Comcast Toolbar is free for all Comcast High-Speed Internet customers.

**PREVENTING IDENTITY THEFT****WHAT TO DO IF YOU THINK YOU MAY BE A VICTIM OF ID THEFT**

If you think your personal information may have been compromised, the FTC recommends taking the following actions as soon as possible to minimize the potential damage from identity theft:

Close compromised credit card accounts immediately.

If someone steals your social security number (SSN), contact one of the three nationwide consumer reporting agencies and place an initial fraud alert on your credit report.

Monitor your credit report for activity.

Consult with your financial institution about any impacts on your accounts.

Contact relevant government agencies to cancel and replace any stolen drivers licenses or other identification documents, and to put an alert on your file.

A vulnerability in Microsoft Excel could allow an attacker to gain control of your computer. Systems Affected:

Microsoft Excel 2003

Microsoft Excel XP (2002)

Microsoft Excel for Mac

Microsoft Excel is included in Microsoft Office. Other versions of Excel and other Office programs may also be affected.

**Solution:** Do not open unfamiliar or unexpected Excel or other Office documents, including those received as email attachments or hosted on a web site.

**06-13-2006: MICROSOFT SECURITY UPDATES**

As part of Microsoft's routine, monthly security update cycle they've released the following [security updates](#).

**SECURITY TIPS****US-CERT: What is Cyberbullying?**

Cyberbullying refers to the practice of using technology to harass, or bully, someone else. Developments in electronic media - email, instant messaging, web pages, and digital photos - add to the arsenal. Computers, cell phones, and PDAs can also be applied to the old practice. Cyberbullying can affect any age group; however, teenagers and young adults are common victims, and cyberbullying is a growing problem in schools. [Dealing With Cyberbullies](#)

**The Basics**

Staysafe.org, an educational site that helps consumers understand a variety of online safety and security issues. Browse the [Staysafe.org Toolbox](#) to learn more about:

[Viruses and Worms](#)

[Scams and Fraud](#)

[Spyware and Adware](#)

[Spam](#)

Watch for signs of identity theft: late or missing bills, receiving credit cards that you didn't apply for, being denied credit or offered less favorable terms for no apparent reason, or getting contacted by debt collectors or others about purchases you didn't make.

#### REPORTING A PHISHING E-MAIL

If you receive an email pretending to be from Comcast, that asks for personal information, this is known as **phishing**. To report a phishing email to Comcast, please:

Forward it to [abuse@comcast.net](mailto:abuse@comcast.net) for further investigation.

Be sure to add the words "phishing email" in the subject field of your email.

Provide full, unmodified header information and the content of the email. Header information is required to determine the true originator of the email. If you are unsure how to extract a full-unmodified header, please visit [www.spamcop.net](http://www.spamcop.net) for instructions.

#### WIRELESS SECURITY

##### Essential Tips for Wireless Security

- Use encryption.
- Turn off identifier broadcasting.
- Change the identifier on your router from the default.
- Change your router's pre-set password for administration.
- Allow only specific computers to access your wireless network.
- Turn off your wireless network when you know you won't use it.
- Don't assume that public "hot spots" are secure.

The Federal Trade Commission is introducing a new section of OnGuard Online at [www.OnGuardOnline.gov/wireless](http://www.OnGuardOnline.gov/wireless) to teach computer users how to protect their personal wireless network connections - and the computers on them - from unauthorized use. The information also is available in Spanish at [www.AlertaenLinea.gov/inalambrico](http://www.AlertaenLinea.gov/inalambrico).

#### SAFETY RESOURCES FOR PARENTS

##### Social Networking - Keeping your Children and Teens Safe

Social Networking is often in the news for all the wrong reasons. Parents can help make online social networking fun and safe for tweens and teens. The FTC offers social networking safety tips, downloadable guides for parents and teens and links to additional online resources. Here is an excerpt from the FTC's *Social Networking Sites: A Parent's Guide*. To learn more about the OnGuard Online Social Networking safety campaign,

#### Is your PC a zombie?

Your innocent, friendly personal computer may be sending out spam to the world... and you may not even know about it. When your PC is hijacked by evildoers to send spam, it is called a "zombie." [Find out how to protect your PC.](#)

#### ANTI VIRUS

##### CURRENT THREATS

[W32/Sdbot.worm!605becc1](#)

[W32/Sdbot.worm!b37e4475](#)

[W32/Bagle.fc@MM](#)

[Downloader-AXA](#)

[Del-507](#)

##### RECENT THREATS

[W32/Breplbot](#)

[Puper](#)

[Exploit-ANIfile](#)

[Exploit-ByteVerify](#)

[W32/Mytob.gen@MM](#)

##### REMOVAL TOOLS

[Lovsan](#)

[Klez](#)

[Bugbear](#)

[Stinger Removal Tool](#)

##### MCAfee ANTI-VIRUS SOFTWARE

[McAfee VirusScan](#)

##### VIRUS SEARCH

[Sign up for email virus alerts from McAfee](#)

##### SECURITY FORUMS



Privacy Statement  
 Terms of Service  
[www.OnGuardOnline.gov](http://www.OnGuardOnline.gov)  
 © 2006 Comcast Cable  
 Communications, LLC. All  
 rights reserved.

While social networking sites can increase a person's circle of friends, they also can increase exposure to people with less than friendly intentions. Here are tips for helping your kids use these sites safely:

In some circumstances, the Children's Online Privacy Protection Act and Rule require social networking sites to get parental consent before they collect, maintain, or use personal information from children under age 13.

Keep the computer in an open area, like the kitchen or family room, and use the Internet with your kids.

Talk to your kids about their online habits. Tell them why it's important to keep their name, Social Security number, address, phone number, and family financial information to themselves.

Your kids should post only information that you and they are comfortable with others seeing and knowing.

Warn your kids about the dangers of flirting with strangers online.

Tell your children to trust their gut if they have suspicions. If they feel threatened by someone or uncomfortable because of something online, they need to tell you, and then report it to the police.

#### HOW DO I?

**How do I prevent spam?**

**How do I run a spyware scan using the Comcast Toolbar?**

**How do I know if my Internet communications are private and secure?**

**How do I secure my wireless network?**

**How do I change my Comcast password?**

**How do I protect my PC from worms, trojans, viruses and other intruders?**

Join the Comcast online community and be a part of the security watch. Report and learn more about the latest spyware, scams and security alerts. [Security Forums](#)

#### SECURITY RESOURCES

##### [New! OnGuardOnline.gov](#)

Be on guard against Internet fraud, secure your computer, and protect your personal information with practical tips from the federal government and the technology industry.

##### [ID Theft](#)

Learn how to protect your identity and what to do if you've been victimized.

##### [Looks Too Good To Be True](#)

Test your knowledge of online fraud and evaluate your level of risk.

##### [GetNetWise](#)

Comprehensive site for information to help you keep your family safe while online.

##### [FTC Consumer Security](#)

Meet Dewey the e-Turtle, who informs you of the latest ways to keep your computer secure.

##### [Microsoft Security Updates](#)

Microsoft releases monthly security updates for manual and automatic download.

##### [Field Guide To Phishing](#)

MailFrontier published a guide to identifying common phishing tactics. Test your knowledge with the Phishing IQ test.

##### [StaySafe.org](#)

Staysafe.org is an educational site intended to help consumers manage a variety of safety and security issues that exist online.

##### [WiredKids.org](#)

An online safety project for kids & teens featuring safety information through online and off-line projects, including Teen Angels, a national network of teen Internet

safety volunteers.

**Netsmartz.org**

The NetSmartz Workshop is an interactive, educational safety resource from the National Center for Missing & Exploited Children and Boys & Girls Clubs of America for children (ages 5-17), parents, guardians, educators, and law enforcement that uses age-appropriate, 3-D activities to teach children how to stay safer on the Internet.

**POLICIES**

**Privacy Statement**

**Subscriber Agreement**

**Acceptable Use Policy**

**Comcast Abuse Policy**

## APPENDIX 2

[Mail](#)
[Radio](#)
[Photos](#)
[Video](#)
[Security](#)
[Sign In](#)
[Ask Comcast](#)

[Web](#)
[Images](#)
[Video](#)
[Shopping](#)
[Help](#)

Search the Web:   [More...](#)

[HOME](#) > [HELP](#) > [FAQS](#) > [SECURITY](#) > [GENERAL](#)
[Go to Express](#)
[Help](#)
[My Account](#)

[HELP:](#) Ask Comcast | [FAQs](#) | [One Click Fixes](#) | [Desktop Doctor](#) | [Help Forums](#) | [Email Us](#) | [Live Chat](#)  
[SECURITY:](#) Anti-Virus | [Personal Firewall](#) | [Privacy Service](#) | [Anti-Spyware](#) | [Security Alerts](#) | [Security Forums](#)  
[MY ACCOUNT:](#) [Reset Password](#) | [Create Additional Email Account](#) | [Enable PWP](#) | [Pay Bill Online](#)

## FAQ

### How can I secure my wireless home network?

Here are 5 quick steps to help you secure your wireless network from unauthorized access. These steps are provided as general guidelines - for detailed help, please contact your hardware vendor. See the bottom of this page for links to some common wireless networking vendors.

1. **Download the latest firmware for your device.**
2. **Change the administrator password.**
3. **Change your SSID and turn off SSID Broadcasting**
4. **Enable WEP**
5. **Limit access by MAC addresses**

Comcast offers a **Wireless Home Networking service**, which includes all of the hardware and software necessary to set up your wireless devices. Comcast Home Networking customers also receive professional installation - including security configuration - along with continuous technical support and remote troubleshooting, 24x7.

1. **Download the latest firmware for your wireless router.**

Firmware is software that's embedded in a hardware device - in this case, your wireless router. The firmware that comes with your wireless router or wireless access point may be out of date. Download the latest firmware to ensure the best security and performance.

As security vulnerabilities are discovered, patches to stop them are developed. These patches are often included in firmware updates. If you're using the default firmware that came with your wireless router, there could be several known security holes that could allow someone to hijack your Internet connection, view the files on each of your networked computers and even steal passwords or credit card numbers.

Most of today's wireless routers allow for firmware updates, and the process is quite simple. Check the web site for your wireless device manufacturer for instructions on obtaining the latest firmware and how to install it. The Linksys support site can be found [here](#) and the Netgear support site can be found [here](#).

## SEARCH HELP

ENTER SEARCH WORD

## RELATED FAQS

1. [As a Comcast High-Speed Internet customer, what do I need to know about Windows XP Service Pack 2?](#)
2. [Blaster Worm Removal Tool for Windows XP and Windows 2000](#)
3. [Can I use SSL with the Comcast newsgroup service?](#)
4. [How do I change my Comcast password?](#)
5. [How do I know if my Internet communications are private and secure?](#)
6. [How do I run a spyware scan using the Comcast Toolbar?](#)
7. [How do I set](#)

## 2. Change the administrator password

Your wireless router's default password should be changed immediately. All wireless routers are shipped with the same administrator user name and password. Changing the user name and password is not only the most important change, it is the easiest. In your wireless router's configuration page, look for a link or setting titled "Admin." If you have any trouble changing this setting, check your wireless router's user guide.

## 3. Change your SSID and turn of SSID Broadcasting

Your wireless router comes with a default SSID (Wireless network name), and one of the first things you should do is change that SSID. By having a non-default SSID, you're making it harder for unauthorized connections to your network.

By allowing your SSID to broadcast, you make it easy to add additional devices to your wireless network. However, you also make it easy for **anyone** with a wireless device to gain access to your network. Leaving broadcasting on is a bit like leaving your car keys in the ignition while you run into the store - you're asking for trouble.

When you turn SSID broadcasting off, your wireless devices will have to be configured with the exact SSID that you have specified in your wireless router.

## 4. Enable WEP

WEP encrypts data both to and from your wireless clients, making it harder for others to peek in on what you're doing. WEP should be enabled, and ideally you should use the strongest key possible, which is usually 128-bit.

## 5. Limit access by MAC addresses

Every network card, both wired and wireless, has a unique address assigned to it from the manufacturer. This identifier is called a MAC address. By setting your wireless router to only allow connections from specific MAC addresses, you're greatly improving the security of your wireless network. For help figuring out what your network card's MAC address is, please see **this FAQ**. Once you know each of the MAC addresses for your network cards, check the support Web site of your wireless router manufacturer for instructions on using MAC address security.

## Common Wireless Networking Hardware Vendors

**Linksys Support**  
**Netgear Support**  
**Microsoft Support**  
**D-Link Support**  
**Motorola Support**  
**Apple (AirPort) Support**

**Windows XP to download and install updates automatically?**

**8. How do I use a credit card on the Internet?**

**9. How secure is the Internet?**

**10. How to protect your PC from worms, viruses and other intruders**

APPENDIX 3



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to  
File No. 305A-BH-47083

1000 18th Street North  
Birmingham, Alabama 35203  
May 30, 2006

Comcast Legal Response Center  
650 Centerton Road  
Morrestown, NJ 08057

RE: Legal Response Team  
Gary Lipscomb

Dear Mr. Lewis:

I would like to bring to your attention the outstanding support your Legal Response Team has afforded the Federal Bureau of Investigation (FBI), specifically, our crimes against children investigators. Their timely responses to our subpoenas are no less than herculean, especially to the scores of victim children who have benefitted from their unselfish and tireless efforts.

In addition to protecting the children of Alabama, your staff's efforts to identify the subjects have also protected the respective law enforcement officers involved in the various undercover activities. Your staff's ability to address our needs on such short notice plays a critical role in our continued success.

In closing, on behalf of the FBI, I would like to express our sincere thanks and appreciation for your unwavering support.

Sincerely,

A handwritten signature in black ink, reading "Dale L. Miskell", is written over the typed name.

Dale L. Miskell  
Supervisory Special Agent



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

Federal Office Building  
Philadelphia, Pennsylvania, 19106  
May 23, 2006

Gary Lipscomb  
Comcast National Security Operations  
Legal Response Center  
650 Centerton Road  
Moorestown, New Jersey 08057

Dear Gary:

It was pleasure speaking with today on several investigative techniques currently under consideration by our office. Your insight is greatly appreciated.

I want to take this opportunity to commend you and your staff for their continued technical and operational support of our mission. Your personal efforts, access and advice are valuable assets and have immeasurably assisted all of us in the law enforcement community sworn to protect the citizens of our local communities and the United States.

We in the Philadelphia Division are particularly grateful for the attention you devote to matters of local interest and importance. I look forward to continuing our excellent business relationship based on the professional trust and confidence we have developed over the last several years.

Sincerely,

*Brain W. Lynch*  
Brain W. Lynch  
Acting Special Agent in Charge

By:  
Edward P. Nowicki  
Supervisory Special Agent  
Technical Operations

To: Lewis, Gerard  
 Subject: RE: Kudos

Sent: Wednesday, June 14, 2006 1:55 PM  
 To: Lipscomb, Gary  
 Subject: Kudos

Dear Gary:

I just want to thank you for your expediency and genuine commitment to assisting us with last night's investigation.

We often are called upon to discover the truth behind claims of child exploitation. Sometimes, there truly is a child at risk, and our joint efforts curb further exploitation. Other times, we reach a dead end, or discover that the claim was false (however well-intentioned it might have been). Either way, your efforts, your record-keeping, and the speed with which you respond, are fundamental to our success.

We get the benefit of following the investigation through to the faces of the victims. You do not. With that, I want to tell you . . . your work makes a difference. By giving us subscriber information, we often reach child predators and other child offenders who, but for your expeditious and diligent record-keeping, would have gone undetected. By improving record-keeping and working together in a courteous efficient fashion, we all can be a part of the administration of justice.

We don't often get "thank yous," and many children, such as those depicted in images of their sexual abuse or solicited through online contacts, have no competent voices to speak on their behalves. But you should know that you have done good. You have impacted the worlds of so many and made this world a better place.

It sounds cliché, but it's true.

Thank you, and keep up the good work.

Sincerely,  
 Dana Leccese  
 ICAC Prosecutor  
 Criminal Bureau  
 Massachusetts Attorney General's Office  
 Boston, MA

6/23/2006

MR. WHITFIELD. Thank you, Mr. Lewis.

And Mr. Reiting, you are recognized for 5 minutes.

MR. REITINGER. Chairman Whitfield, Representative DeGette, and members of the subcommittee, my name is Philip Reiting.

Thank you for the opportunity to appear before you today to talk about Microsoft's strong commitment to protecting children.

I am Microsoft's Director for Trustworthy Computing in Washington, DC, but before joining Microsoft, I was the Deputy Chief of the Computer Crime Intellectual Property Section at the U.S. Department

of Justice and the Executive Director of the Department of Defense's Cybercrime Center. For years, I have been concerned with the challenges posed in preventing, detecting, deterring, and investigating cybercrime.

Microsoft is deeply and broadly engaged in efforts to protect children on the Internet. My written testimony discusses those efforts in detail.

As a former law enforcer, I believe that among the most critical are our efforts to partner with law enforcement to better enable it to prosecute child exploiters and predators. We must ensure that those who harm our children are caught, prosecuted, and sent to jail.

As a technology leader, Microsoft understands and embraces its obligation to partner with law enforcement to protect kids. We began by working to expunge child pornography from our systems and identify violators to law enforcement. We use filters on images uploaded to MSN spaces and groups to identify possible pornography. The images that are flagged are reviewed, and if they appear to be child pornography, an instant report is sent to the National Center for Missing and Exploited Children. MSN closes the site and preserves it for a period in anticipation of legal process.

We also work to respond rapidly to law enforcement investigations. Our compliance managers are on duty 24 hours a day, 7 days a week to respond to requests from law enforcement regarding criminal violations.

Our efforts to support prosecutions, however, do not stop there. In 2003, Toronto detective, Sergeant Paul Gillespie, wrote to Bill Gates asking for his help. In response, Microsoft began developing the Child Exploitation Tracking System, or CETS, an innovative tool that enables law enforcement to track and share information in child exploitation cases. It has been incredibly rewarding to hear from our colleagues in Canada that CETS has already played a role in several investigations across geographical boundaries, creating links that have helped apprehend over 40 online predators,, and most important, led to the rescue of children in countries around the world. Microsoft is also working closely with several other law enforcement agencies around the world to assist with additional deployments.

We are deeply involved in training law enforcement. In just one example, in April of 2004, Microsoft joined Interpol and the International Center for Missing and Exploited Children to launch the international center's global campaign against child pornography under which Microsoft has trained nearly 1,500 law enforcement officers from 91 countries.

And as has already been discussed by several of the members of this panel, we are pleased to announce that Microsoft has joined with the



National Center and a number of companies represented on this panel to establish the Technology Coalition. We are convinced that this partnership will make a meaningful contribution to protecting our children from Internet predators and inappropriate online material.

Of course law enforcement prosecutions do not provide a silver bullet for child exploitation. To stop child exploitation before it can occur, we also work to empower families and communities to protect their children through both education and technology. We provide safety information on our sites and partner with many groups to educate families about how to protect themselves.

Again, our efforts are described in detail in my written testimony, and I won't repeat them here.

We also continue to invest heavily in building technologies to protect kids and give parents the ability to better manage a child's use of technology, including filtering, family safety settings, and safe search capabilities. The soon-to-be-released Windows Vista operating system will go even farther and allow detailed control over games, time, applications, and browsing. And Windows Live family safety settings will offer a similar free web-based protection.

In conclusion, Microsoft is strongly committed to improving online security for children throughout the world and to supporting investigation, prosecution, and punishment of child exploiters and predators. Microsoft and its partners are in the process of developing and implementing best practices for protecting children, and we welcome your feedback about how we can do better.

Thank you for the opportunity to speak with the committee about this important topic. I look forward to answering your questions.

[The prepared statement of Philip R. Reiter follows:]

PREPARED STATEMENT OF PHILIP R. REITINGER, SENIOR SECURITY STRATEGIST,  
MICROSOFT CORPORATION

Chairman Whitfield, Ranking Member Stupak, and Members of the Subcommittee, my name is Philip Reiting. I am the Director for Trustworthy Computing in Washington, D.C. for Microsoft Corporation. Thank you for the opportunity to appear before you today to underscore Microsoft's strong commitment to protecting children from online predators and inappropriate material, and the steps we have taken to increase online safety. Before joining Microsoft, I was a Deputy Chief of the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice, the Executive Director of the Department of Defense Cyber Crime Center, and the Chair of the G8 Subgroup on High-Tech Crime. For much of my career I have been concerned with criminal online threats, and the challenges posed in preventing, detecting, deterring, and investigating cybercrime.

Microsoft is deeply and broadly engaged in efforts to protect children from Internet predators and inappropriate online material. Our efforts are focused in three general areas: (1) partnering with law enforcement to identify online threats to children and enable law enforcement to investigate and prosecute those who abuse or exploit them through the online environment, (2) empowering families through technological advances in our products and services to educate and protect their children, and (3) partnering with citizens, other companies, organizations, and government to educate communities more broadly regarding the risks to children in online activity and ways to keep them safe. In brief, Microsoft works with our partners to prevent child exploitation online, and actively supports law enforcement efforts in the U.S. and around the world to prosecute and punish those responsible for these heinous crimes.

Partnering with Law Enforcement to Identify, Investigate and Prosecute  
Child Pornography and Exploitation

As a technology leader, Microsoft understands and embraces its obligation to partner with law enforcement to combat child pornography and exploitation. When criminals harm children, online or offline, they must be caught, prosecuted, and punished. Microsoft views its partnership with law enforcement as critical to its efforts to protect children. First, Microsoft operates its online services so as to detect and prevent child pornography and exploitation, and works with law enforcement in its investigation of criminal acts. Second, Microsoft provides law enforcement specialized technology to help uncover, prosecute and convict criminals, and training to enhance its capabilities.

Abuse Detection and Reporting: MSN uses a filtering tool to review images uploaded to MSN Spaces and MSN Groups. Images that the filtering tool flags as potential child pornography are reviewed and, if child pornography is apparent, an incident report is sent to the National Center for Missing and Exploited Children (the National Center), pursuant to the requirements of the 1990 Victims of Child Abuse Act (1990 Act). Microsoft also follows the sound practices of the United States Internet Service Provider Association (USISPA) in reporting the facts or circumstances of apparent child pornography to the National Center, including providing samples of the images uploaded. Upon receiving this report, the National Center notifies law enforcement as provided in the 1990 Act. MSN closes the site and preserves the entire site, account information and associated files in anticipation of legal process

Microsoft also maintains a customer/user complaint capability, to review reports of child pornography or exploitation. When the central abuse handling support center confirms an apparent incident of child pornography or exploitation, it takes down the

offending site and reports the incident to the National Center using the procedures described above.

Responding to Law Enforcement Requests: Microsoft's reports to the National Center set in motion a process under which law enforcement will request that Microsoft provide evidence of the criminal acts reported. Law enforcement also seeks evidence of child exploitation from Microsoft based on information law enforcement receives from other sources. Microsoft's compliance managers are on duty 24 hours a day 7 days a week to respond to requests from law enforcement to preserve or disclose evidence regarding criminal violations. Our compliance officers also educate and train U.S. and foreign law enforcement in how to obtain evidence from Microsoft regarding those engaged in child exploitation or pornography, consistent with U.S. law and privacy protections. Training law enforcement allows for better evidentiary requests and expedites law enforcement's process flow in collecting evidence.

The Child Exploitation Tracking System (CETS): In addition to providing to law enforcement evidence of criminal acts involving contacts with children online, Microsoft has developed technology to assist law enforcement in detecting, prosecuting and convicting child predators. In 2003, in response to a request to Bill Gates from Toronto Police Officer Detective Sergeant Paul Gillespie, Microsoft began developing CETS, an innovative, open standards-based software tool that enables law enforcement to better gather and share evidence of online child exploitation over a secure system based on legal agreements in place. CETS permits investigators to easily import, organize, analyze, share and search information from the point of detection through the investigative phase to arrest and conviction. The CETS system has now been adopted by law enforcement agencies across Canada. It has been incredibly rewarding to hear from our law enforcement colleagues in

Canada that the CETS already has played a part in several investigations across geographical boundaries, creating links that have helped apprehend over 40 online predators and, most importantly, led to the rescue of children in countries around the world. Microsoft also is working closely with several other law enforcement agencies around the world to assist with additional deployments to build a truly global network. To date, Microsoft has committed over \$5 million to create the system and to help international police adopt and implement it.

Additional Support for U.S. Law Enforcement: Microsoft also sponsors federal, state and local law enforcement forensic and technical training programs to assist officers in cybercrime and child protection investigations, and continues to explore new opportunities to provide additional training of law enforcement officials. Microsoft also works closely with state Attorneys General in Florida, Georgia, New York, South Carolina, Texas, Washington and other states across the U.S. to develop tools and training and to provide technical support to investigations and prosecutions for online child exploitation and other cybercrimes.

Support for Foreign Law Enforcement and Global Cooperation Efforts: The Internet is a global environment and child exploitation is, sadly, a global tragedy. Helping to assure the online safety of children demands that Microsoft work around the globe, and within the law, to help protect users from inappropriate content, whatever its origin, and to help police around the world lawfully to apprehend child exploiters wherever they may be. Our efforts here include developing and deploying CETS and additional activities described below.

Global Campaign Against Child Pornography: In April 2004, Microsoft, Interpol and the International Centre for Missing and Exploited Children (International Centre) jointly announced the launch of the International Centre's Global Campaign Against Child

Pornography. As part of this campaign, Microsoft has contributed \$1.5M to develop and implement a global training program for law enforcement. The training – known as the Computer Facilitated Crimes Against Children seminars -- consists of a series of four-day conferences designed to educate law enforcement officers around the world on identifying and investigating online criminal conduct against children; how to interact with victims and prevent further abuses; key issues such as human rights, data protection, and compliance with national laws; and managing complex international investigations. As of June 2006, 1,490 law enforcement officers from 91 countries have been trained in 16 regional training sessions in Europe, Central and South America, South Africa, Europe, Asia, and the Middle East.

Roundtable Discussions on Children's Online Safety: In addition to the training with the International Centre, Microsoft has sponsored a series of roundtable discussions on Children's Online Safety issues in countries around the world. These dialogues have brought together law enforcement officials, policymakers, industry experts and community leaders to examine how to stop illegal and harmful Internet activities targeting minors and small children, and to share best practices and lessons learned. The roundtables typically include panels examining the scope of the problem of online child exploitation and address child online safety from both public and private sector perspectives.

Virtual Global Task Force (VGTF): Through the VGTF, Microsoft has partnered with U.K., Australian, and Canadian law enforcement officials to develop a police reporting and patrol website and other initiatives. Additionally, the MSN Online Safety and Security site features a link to the VGTF Web site allowing individuals to report potentially illegal content.

CAN-SPAM and Efforts to Eliminate Spam: Microsoft's ongoing efforts against spam help to make the Internet safer for children because spam often contains links, messages and images not appropriate for children. Microsoft and other leading IT companies have partnered with enforcement officials worldwide to bring successful actions against unlawful spam. In addition, in March 2004, Microsoft and three other large Internet service providers — America Online, Earthlink, and Yahoo — filed multiple complaints in federal courts in the United States against hundreds of defendants for violating the CAN-SPAM Act, an important law that originated in the House Energy and Commerce Committee. Likewise, in September 2004, Microsoft joined with Amazon.com to file several lawsuits against chronic spammers who had targeted consumers by spoofing domains and phishing for consumers' personal information. In total, Microsoft's efforts to enforce anti-spam laws have produced more than 190 legal actions worldwide — with enforcement efforts in Asia Pacific, Europe and the Middle East, and the United States — and have resulted in approximately \$869 million in legal judgments against spammers.

Cybercrime and Digital Forensics Workshop: On April 19-22, 2005, Microsoft and the Asian Development Bank Institute co-hosted an International Workshop on Cybercrime and Digital Forensics in connection with the 11<sup>th</sup> UN Congress on Crime Prevention and Criminal Justice. The workshop, developed for cybercrime investigators from countries across the Asia Pacific region, included practical, hands-on training from Microsoft specialists on the latest techniques in combating a range of computer crimes, including child exploitation.

Council of Europe Convention on Cybercrime: Microsoft has joined partners in industry to encourage countries, including the United States, to adopt and ratify the Council of Europe Convention on Cybercrime (COE Convention). The COE Convention is a

powerful international instrument on cybercrime and is increasingly viewed as the global standard for criminalization obligations and governmental cooperation in this area. The COE Convention provides an important baseline for effective international cybercrime enforcement by requiring signatories to adopt and update laws and procedures to address crime in the online environment, and by providing for mutual investigative assistance between signatories. Notably, the COE Convention requires signatory nations to adopt laws criminalizing the production and distribution of child pornography through a computer system.

Financial Coalition Against Child Pornography: In March 2006, Microsoft joined the National Center and the International Centre and 16 of the world's leading financial institutions and other Internet industry leaders to form the Financial Coalition Against Child Pornography. The Coalition provides a forum for members to collaborate on a multi-pronged strategy with the objectives of closing down funding for child pornographers and eradicating commercial child pornography by 2008.

Model Legislation Against Child Pornography: In April 2006, Microsoft joined the International Centre in announcing support for model legislation against child pornography, and pledged to help pursue enactment of such legislation worldwide.

Safe Computing Program: Microsoft Canada and the University of Toronto's Center for Innovation Law and Policy launched the "Safe Computing Program" in 2005 to help in the fight against online child sexual exploitation. Microsoft Canada provided funding to the Centre for research and worked with the Office of the Attorney General (Ontario) in developing new policies.

INHOPE: Through software donations and training, Microsoft also supports INHOPE, the International Association of Internet Hotlines. INHOPE is a European



Union-supported organization with 23 member hotlines in 21 countries that responds to reports of illegal content to make the Internet safer.

#### Providing Safety Technology and Tools to Families

While partnerships with law enforcement are a critical component of efforts to protect children, empowering families to manage risk is equally important. We at Microsoft are committed to arming parents and guardians with both information to educate their children about online risks and technological tools to reduce such risks.

We continue to invest heavily in technologies that make computing more secure and the Internet experience safer for everyone. Tools we develop are made available globally in localized versions to enhance online security throughout the world. Our security and Internet safety efforts are driven by our Trustworthy Computing Initiative, which launched in 2002 and initiated a company-wide, top-to-bottom commitment to enhance the security and privacy of online users. At its heart, Trustworthy Computing is a long-term effort to create a secure, private and reliable computing experience for everyone and to increase user confidence in information technologies. Trustworthy Computing includes: support for the development of strong laws addressing criminal online conduct; support for law enforcement training, investigations, coordination and prosecutions; and encouraging and helping customers to adopt security best practices.

To assist parents in promoting online safety, Microsoft offers, and is investing in further development of, a variety of family safety technologies and tools. These tools employ user-friendly interfaces to make it simpler to act safely online, to help protect their personal information, and to permit parents and guardians to make and enforce informed and specific choices and to access activity reports about the Internet site visits their children

made and the content to which they were exposed. These tools include both features of our web services, such as MSN Spaces, and family safety tools in the operating system and available for free from Windows Live. These family safety tools help families customize both their PC and their Web-based protection.

MSN: MSN Spaces, for example, allows users to create their own weblog, or *blog*, and invite others to view photos and messages. MSN Spaces employs strong abuse prevention and detection processes. In addition to the filtering capabilities referenced above, upon signing on to MSN Spaces, the user is warned in the Terms of Use and Code of Content that illegal uses of the technology are prohibited. The Code of Conduct expressly and prominently prohibits uploading, posting, transit, transfer, dissemination or distribution or facilitation of any content, including text, images, data, sound or software that is intended to harm or exploit minors, is illegal or violates local or national laws, including child pornography. See <http://spaces.msn.com/coc.aspx>. Other MSN properties have similar terms of use.

MSN Spaces is also designed with safety and privacy in mind. MSN Spaces' social networking features are designed to support developing closed networks of friends, not building networks of tens of thousands of unknown people. To complement user education, MSN Spaces also includes a number of features designed to enhance safety. For example, use of MSN Spaces requires that users have a Microsoft Passport. Offensive terms filtering is employed at the user name/alias and sub-title level, and privacy and communications preference controls are included. MSN Spaces also provides safety information, and information about how to set viewing and contact permissions directly on the MSN Spaces site and during the set up process for a Space. We recommend that all users keep personally identifying information to themselves, exercise care when posting

photos with personal details, and never meet an Internet contact in person alone. MSN Spaces' safety tips also include a link to the short cautionary film "Predator," which a 14-year old boy wrote, directed and filmed working with his local police department.

[http://staysafe.org/teens/student\\_spotlight/predator.html](http://staysafe.org/teens/student_spotlight/predator.html).

In addition, MSN9 Premium Parental Controls incorporate content-filtering technology and offer several features that are designed to help parents manage their children's use of the Internet, while helping to protect them online. MSN Search offers a SafeSearch feature to filter sexually explicit content, and MSN contains pages developed specifically for kids.

Windows Vista: Through parental controls in our soon-to-be-released, next-generation Windows Vista operating system, parents will be able to control games played on a PC; establish time limits for how long their children use the computer; set gaming, application, Instant Messaging and Web restrictions; and receive logging and activity reports on their children's PC use. These controls will be easy to use yet allow detailed control – web browsing, for example, can be filtered by the type of content found on a web page. Windows Vista, as an open platform, will also enable users to run their choice of family safety software, and we anticipate working with a number of partners to enhance the family safety of the Windows Vista computing experience.

Windows Live Family Safety Settings: A free web service which will be available this year through the Windows Live set of online services, Windows Live Family Safety Settings was built to put better filtering tools in the hands of parents and guardians. By making these tools available for free, Microsoft is leading the industry in providing additional steps to enable parents and guardians to protect kids. Windows Live Family Safety Settings will provide web content filtering, including filtering of chat and mail; customized allow and

block lists; customized approve/disapprove contact lists for Windows Live Instant Messenger (IM), MSN Spaces and Windows Live Hotmail; a kids request line that allows a parent to unblock a website in real time; roaming access to settings and activity reports on the web; and guidance for parents and kids from third party experts like the American Academy of Pediatrics. Windows Live Family Safety Settings will roll out in phases beginning this summer.

Xbox 360 and Xbox Live: Xbox 360 provides Family Settings worldwide to permit age-appropriate offline and online entertainment. Parents can restrict the games and DVD movies the console will play (based on established ratings systems, such as ESRB in the U.S.), as well as whether or not their children may create an Xbox Live account to play and communicate with fellow gamers online. The console's Family Settings apply to all users, so any game whose content surpasses the threshold set by the parent will not play unless a parent enters a secret code they have created. The Xbox Live Family Settings can be customized for each child in the family, and each child's personalized restrictions apply when the he or she plays Xbox away from home. Xbox Live Family Settings enable parents to control which friends may be added to the child's list of online contacts; disclosure of the child's online status; allowable communication methods, for example, whether the child can communicate via voice, video, or text messages; whether the child's gamer profile may be viewed by others and whether the child may view others' profiles; and game content (user-created or purchased content). Default settings are provided for children 12 or younger and ages 13-17. . In addition, Microsoft's guiding principles prohibit the functionality of certain game content (e.g., Microsoft does not manufacture or license others to create "adults-only" or sexually explicit games to run on Xbox consoles, and unlicensed game disks simply will not run, regardless of their content). See <http://www.xbox.com/en->

[US/support/familysettings/20051118-entertainmentcitizenship.htm](http://US/support/familysettings/20051118-entertainmentcitizenship.htm). These investments earned Xbox Live the WiredKid's Safe Gaming Award in both 2003 and 2005.

Additional Safety Information: Microsoft has a wide range of safety and security information available on the various company and product websites. Microsoft.com - [www.microsoft.com/athome/security](http://www.microsoft.com/athome/security), as well as websites for MSN - <http://safety.msn.com>, and for Xbox - <http://www.xbox.com/en-US/support/familysettings/default.htm>, provide information about online risks, training materials and tools to prevent safety issues.

We recognize that parents cannot always watch over their child's shoulder when he or she is on the computer. These parental tools directly address child online exploitation and child safety by giving parents the ability to better understand what their children are doing online, to shape and direct a child's online experience, to help generate productive conversations with children about safe behavior, and to manage the child's use of the Internet and the personal computer. For example, the ability to block a specific website – or category of websites – enables parents to put web chat or social networking sites on hold until they are sure their children understand and follow safety rules.

Moving forward, we will continue to invest in family safety innovation to enhance the protection offerings for our customers of the MSN network, Xbox 360 and Xbox Live, and our new Windows Live services.

#### Partnerships to Educate Communities About Child Online Safety

In addition to educating parents, Microsoft works to educate communities across the country and the world about risks to children online and tools to reduce these risks. The following provides a sampling of our efforts in this area.

GetNetSafe: A coalition of technology companies, educational organizations, government and advocacy groups<sup>1</sup> have joined together to support a national tour to raise awareness of computer security and Internet safety. During the 2006 tour of 12 U.S. cities experts will visit school assemblies and parents' nights, local community and senior events, business luncheons and Internet fairs to provide the information and tools communities need to protect themselves and their children. The tour will visit Washington DC, Boston, Phoenix, Dallas, Chicago, Detroit, New York City, Philadelphia, Charlotte, Los Angeles, Seattle, and Orlando.

Stay Safe Online and GetNetWise: Microsoft is a member of the National Cyber Security Alliance (NCSA), which is a partnership between the private sector and the Department of Homeland Security and the Federal Trade Commission to promote safe computing and the October "National Cyber Security Awareness Month" activities. The NCSA website, [www.staysafeonline.info](http://www.staysafeonline.info), has helpful material and information and tips about how to promote a more safe online computing experience for children and parents. These materials are available for use by anyone in the public or private sector who wants to help educate consumers. Microsoft also provides similar and supporting information.

In addition, Microsoft and several other leading technology companies, including AOL and AT&T, launched GetNetWise ([www.getnetwise.org](http://www.getnetwise.org)) as an online industry resource for parents and childcare providers. GetNetWise educates parents about the potential risks to children on the Internet and offers parents suggestions on how to interact with children regarding these risks. Additionally, GetNetWise provides parents with

---

<sup>1</sup> The Get Net Safe project was created by 12 partners, including: the Federal Trade Commission, the Department of Commerce, AARP, the National Center for Missing and Exploited Children (NCMEC), the U.S. Chamber of Commerce, i-SAFE America, RSVP, Boys and Girls Clubs of America, GetNetWise/Internet Education Foundation, National Cyber Security Alliance (NCSA), Microsoft Corporation and Best-Buy/Geek Squad.

information on the wide variety of available technological tools that can help limit children's access to inappropriate content and communications on the Internet.

Get Safe Online: Microsoft also is a major sponsor of the U.K.'s recently-launched "Get Safe Online" Internet Security campaign. As part of that campaign, we worked with the VGTF and ChildNet International to create an educational program for children, teachers, and parents entitled "Getting to Know IT All." As part of this pilot program, 175 Microsoft employees have been volunteering as trainers in schools and community centers around the United Kingdom teaching thousands of young people how to stay safe online.

#### Conclusion

Microsoft is strongly committed to improving online security for children and all our customers throughout the world, and to supporting investigation, prosecution, and punishment of child exploiters and predators. Through close partnerships with law enforcement, government officials and NGO's around the world, as well as technological advancements and parental education, we continue to make strides in combating online threats to our children. Through these means, Microsoft and its partners are in the process of developing and implementing best practices for protecting children.

Of course, in a field as important, rapidly changing, and complex as this one, there is always room for improvement, and we welcome feedback. Just as criminals find new ways to harm children, the good guys must be equally agile, working closely together to evolve methods for tracking and capturing child predators. To achieve such agility, there must be a global commitment to well-organized collaboration among policymakers, law enforcement, the NGO community, and industry. We at Microsoft will continue to look for new and innovative ways to collaborate with law enforcement, government officials at all levels, and

other key participants in the fight against child exploitation, pushing the boundaries through technology solutions, and user education.

Thank you for the opportunity to speak with the Committee about this important topic.

MR. WHITFIELD. Thank you, Mr. Reitingner.  
And Ms. Wong, you are recognized for 5 minutes.



MS. WONG. Thank you, Mr. Chairman. And thank you, Representative DeGette and the members of the subcommittee, for inviting me to participate in this important discussion about how to keep all of our children safe.

My name is Nicole Wong, and I am Associate General Counsel for Google responsible for our products and services, including the privacy, security, and safety of our users.

I am also the mother of two young children, and I appreciate the subcommittee's leadership on this important issue of concern to all of America's families.

As a company, Google is deeply committed to protecting children on the Internet in our actions and in our guiding principles. Child pornography is a horrific and vicious crime and has no place in a civilized society. Google has a zero-tolerance policy for child pornography and those who would promote it. When we become aware of child pornography anywhere in our search index or on our site, we remove it immediately and report it to the appropriate authorities. We do not accept any advertising related to it. We cooperate assiduously with law enforcement to help track down online criminals and child predators.

We believe that a successful approach to combating child exploitation online must encompass three elements: first, strong law enforcement efforts to pursue and convict the purveyors of illegal content and activity; second, powerful technology solutions and resources for families to control their online experiences; and third, strong industry practices that support all of these important efforts.

At Google, we are approaching a number of initiatives. First, we enforce a strict policy prohibiting any advertising related to child pornography. We do this through a multi-tiered review process that involves both automated checks and manual reviews by trained specialists. We work constantly to improve this process to keep up with the fast-changing jargon and practices of this unsavory industry. In fact, based on the very helpful input of the committee staff, we recently tightened our review program to refuse any ads promoting pornography with teens, even if the underlying websites lawfully depict adult models.

Second, we remove and report child pornography immediately when we become aware of it in our search engine or in any of our websites. Indeed, we have created multiple channels throughout the company to identify illegal material, which includes training teams in our engineering, product, and advertising groups to identify and report instances of child pornography whenever they find it.

We have also created paths for our users to report illegal material to us through the Google Help Center, and we are members of international industry associations, such as the Internet Watch Foundation in the UK,

from whom we obtain lists of illegal websites and use those to block illegal websites. There is a specially trained team in the legal department that submits reports of this material to the appropriate authorities, including the National Center for Missing and Exploited Children.

Third, we provide valuable support to law enforcement at the Federal, State, and local levels. We have a trained and dedicated staff for responding to all law enforcement requests. They are available 24/7, 365 days a year. We are extremely proud of this team that works relentlessly to respond to every law enforcement and data preservation request, including the hundreds of child safety requests we receive each year.

Fourth, we work to empower families to be safe online in a number of ways. We create tools, like our safe search filter, that allows families to control the type of information accessible through our site. We work with our industry colleagues, including those at the table today, and also in forums, such as the Financial Coalition Against Child Pornography, to establish best practices and other initiatives to combat child pornography. And we support efforts like the Wired Safety Educational Campaign and specifically, they work in broad-based education for parents, community police officers, and kids themselves to learn about how to stay safe on the Internet.

The Internet provides an unparalleled opportunity for people to connect with information, and Google's mission is to make this information more accessible and useful. At the same time, we keenly understand that our business relies on the existence of a healthy and trusted Internet. Child pornography and those who purvey it should have no place in that ecosystem.

We look forward to working with you, the law enforcement community, and the broader Internet community to increase our efforts to stop child exploitation and preserve the Internet as a trusted and safe environment.

Thank you.

[The prepared statement of Nicole Wong follows:]

PREPARED STATEMENT OF NICOLE WONG, ASSOCIATE GENERAL COUNSEL & CHIEF  
PRIVACY OFFICER, GOOGLE, INC.

*1. Summary and Introduction*

Mr. Chairman and Members of the Subcommittee, thank you for this opportunity to present Google's perspective on "Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites." We appreciate the Subcommittee's leadership in addressing an issue of such great concern to America's families.

Google has a zero-tolerance policy when it comes to child pornography and those who would promote it. Child pornography is illegal around the world and has no place in a civilized society. When we become aware of child pornography anywhere in our search engine index or on our site, we remove it immediately and report it to the appropriate authorities. We do not accept any advertising related to it. We cooperate assiduously with law enforcement authorities to help track down online criminals and child predators. As a company, in our actions and in our guiding principles, we are deeply committed to protecting children on the Internet.

We believe that a successful approach to combating child exploitation online must encompass three elements:

- Strong law enforcement efforts to pursue and convict the purveyors of illegal content and activity;
- Powerful technology solutions and other resources for families to control their online experiences, according to individual values; and
- Strong industry practices that support these efforts.

Google is pursuing this approach through a number of initiatives:

- We enforce a strict policy prohibiting any advertising related to child pornography.
- We remove child pornography immediately when we become aware of it in our search engine or in our websites. We also report it to the appropriate authorities, including the National Center for Missing and Exploited Children (NCMEC).
- We provide valuable support to law enforcement efforts, by responding to hundreds of child safety-related requests per year, as well as data preservation requests.
- We empower families to be safe online with tools like our SafeSearch filter and our support for efforts like the WiredSafety educational campaign.

The Internet provides an unparalleled opportunity for people to connect with information and with each other. Google's mission is to make such information more accessible and useful. But as we all aware, some online activities can pose risks to children and families, and some online behavior violates the law and should be eradicated. Much can be done to combat these risks, consistent with the open character of the Internet and the diversity of individual family values.

We look forward to describing the ways in which Google is working today – and we look forward to working with you, the law enforcement community, and the broader Internet community to increase our efforts to stop child exploitation and preserve the Internet as a trusted and safe environment.

2. *Industry Practices Combating Child Pornography*

Child pornography is a horrible crime. It has no place on the Internet nor in our users' search experience. As we describe below, we strictly prohibit the advertisement of child pornography in our AdWords program and use both automated and manual filtering techniques to detect and report individuals who attempt to advertise such material. We also report all instances of child pornography to the appropriate authorities as soon as we become aware of it in our index or on any of our websites.

a. *Google Standards for Advertising*

We devote significant resources to detecting and reporting child pornography that someone may attempt to advertise through our ads service.

To explain our service generally, Google's AdWords service allows any potential advertiser – from a neighborhood dry cleaner to a Big Three automaker – to easily create text-, image-, or video-based ads and to display them online in a targeted manner. AdWords is principally a self-managed program, meaning that most advertisers create and control their advertisements through an online interface. Google has hundreds of thousands of advertisers, with millions of ads being displayed in any given month. Screening these ads is a challenge we take very seriously.

Google recognizes that the success of any of our products ultimately depends on quality. We have therefore implemented rigorous quality standards for advertisements submitted through AdWords. In keeping with our company values and mission, Google has policies restricting the types and content of advertising we accept. The AdWords service employs numerous automated and manual checks, program policies, and enforcement mechanisms to assist in providing our users, publisher partners, and advertisers with advertising services that are high-quality and relevant.

As a starting point, our AdWords program Content Policy explicitly states that “[a]dvertising is not permitted for the promotion of child pornography”. The policy is available online at <https://adwords.google.com/select/contentpolicy.html>. The Terms and Conditions for AdWords, available online at <https://adwords.google.com/select/adsandcsfinder>, requires users to agree that they will not use the service to advertise anything illegal.

We enforce our Content Policy through a screening process that combines automated and manual review. The AdWords system begins performing automated policy checks as soon as an advertiser submits an ad. Text ads entered through our online system are subject to real-time automatic screening for potentially sensitive or objectionable terms. If the ad and the list of associated keywords are flagged in this automated screening process, the ad is subjected to further review by the Google AdWords team, and will not appear anywhere until it has been reviewed and approved by a team of trained employees. All ads flagged as relating to adult content are manually reviewed by our trained specialists.

Thanks in part to input we received from this Subcommittee's staff, we recently revisited the issue of how we treat ads referencing teen pornography. We want to ensure that advertisers, even if they may offer completely lawful material, are prohibited from making allusions to illegal content in advertisements to attract customers. To this end, we've enhanced our policies to prohibit the promotion of underage teen pornography.

As we stated earlier, advertisements promoting child pornography are strictly prohibited. When we discover an applicant we suspect is engaged in child pornography, we immediately report the case to the appropriate authorities, such as NCMEC. In our experience, child pornographers very rarely attempt to

advertise online as it requires the submission of verifiable personal information, including a credit card. We estimate that we identify and report to the authorities approximately one to two advertisers every six months whom we suspect are engaged in child pornography.

*b. Reporting & Removal*

Google immediately removes images of child pornography as soon as we become aware of the existence of child pornography on any Google website. We also immediately report it to the National Center for Missing and Exploited Children ("NCMEC"), along with identifying information for the individual who posted the material.

In addition, when we become aware of child pornography on any Internet website that appears in our search results, we immediately remove the link to such a website from our search results and report the site to the appropriate authorities.

Google has developed a variety of methods of detecting child pornography that may appear in our services.

First, we train our employees to recognize child pornography and to report it to our legal department. Specifically, the customer support representatives who work on products that involve user-submitted material receive such training. Members of our web search quality team are also trained to recognize child pornography when they find it in our index. Employees are trained to regularly report any child pornography that they detect to our legal department.

Second, we receive information about websites containing child pornography through our membership in international industry associations, such as the Internet Watch Foundation (IWF) in the United Kingdom and The Association for the Voluntary Self-Monitoring of Multimedia Service Providers (abbreviated FSM) in Germany. In addition to supporting these groups' advocacy work, we routinely access their databases that list websites suspected of containing child abuse images and remove any illegal URLs from our search results.

Third, we encourage our users to tell us about inappropriate content they may encounter in our products and services through the Google Help Center.

When our employees find or receive information about images of child pornography through any of these sources, they immediately report it to the legal department. Our legal department has a team of people trained to submit reports to authorities such as NCMEC and they make daily reports using the organization's web-based reporting tool.

*c. Industry Coalitions*

In addition to its own initiatives for detecting and reporting child pornography, Google is increasingly involved in private-sector initiatives devoted to combating child pornography. For example, Google recently joined the Financial Coalition Against Child Pornography, a group of financial institutions and Internet companies working together to stop the online purchase and exchange of child pornography. The goal is to eradicate commercial child pornography by 2008.

We look forward to engaging with others in the industry and with NCMEC through the Financial Coalition and other initiatives. We are hopeful that these collaborative industry efforts will result in the development of new methods of eradicating the use of the Internet for the crime of child pornography.

### 3. Promoting Child Safety on the Internet

Google recognizes that parents and children around the world use Google.com as an educational tool to explore the Internet and discover the world's information. We are proud of that use of our service.

Google also recognizes the risk that children who use the Internet may come across material that may be inappropriate because of the content of the material, their age, their family's values, or a combination of these factors. Google believes that technological tools and user awareness are among the most effective means of promoting child safety on the Internet.

#### a. *Tools for Safe Searching*

Google believes that technological tools are an important method of protecting children from inappropriate content on the Internet in a way that reflects the needs of individual families. As such, Google has developed its Safe Search tool, which is available to any user of Google.com who wishes to filter adult content from search results.

Google's SafeSearch is an automated tool that screens for websites containing explicit sexual content and removes those websites from search results based on the SafeSearch setting chosen by a user. The SafeSearch filter uses advanced technology to check keywords, phrases, URLs and Open Directory categories, to block pornographic and other explicit sexual content from search results. No filter is 100% accurate, but we believe that SafeSearch effectively eliminates most inappropriate sexual material. Users can customize their SafeSearch settings by clicking on the "Preferences" link to the right of the search box on Google.com, and selecting one of the following:

- **Strict filtering**, which applies SafeSearch filtering to both image search and ordinary web search results;
- **Moderate filtering**, which excludes most explicit images from Google Image Search results, but does not filter ordinary web search results. This is the default SafeSearch setting for users of Google.com, who may change the setting as desired; and
- **No Filtering**, which turns off SafeSearch filtering.

Experience has shown that filtering controlled by end users tends to be one of the more effective and flexible approaches to limiting exposure to unwanted content. Other methods, such as attempting to block whole search requests, can prevent users from finding useful resources associated with blocked terms. (For example, blocking searches for "child pornography" would prevent a user from finding information about NCMEC and other child protection resources.) Blocking specific searches also tends to be ineffective against sophisticated users who simply revise their search terms to evade blocking. Other methods, such as imposing a single standard for all users, can overblock content for some while providing insufficient protection for others.

We are constantly seeking new and better ways to ensure our users see the best lawful results we can find. We believe filtering technologies, like SafeSearch, are powerful tools for families to manage the information available on the Internet, according to their own values and the needs of their children.

#### b. *Promoting User Education*

Educating America's families about how to be safe online remains one of the most important initiatives in the area of child safety. Great work is now being done to better equip parents and children, from tips

about where to put computers in the home (for example, where parents can see them) to online safety curricula that teach children how to avoid predators and unsafe content.

Google applauds the many private-sector organizations devoted to child safety issues on the Internet, and supports their causes. For example, earlier this month, Google co-sponsored WiredSafety.org's first annual "Protecting Our WiredKids" Internet Safety Summit in White Plains, New York. The Summit focused on social and community networking websites and best practice models in that emerging Internet space. We are also excited about a new project to help WiredSafety develop Internet safety educational materials to be used by local community policing officers, including lesson plans, activities and student presentation materials.

In addition, Google is pursuing opportunities to provide free public-service advertising to government agencies and non-profit groups in support of public education campaigns about child online safety. Google believes that these and other initiatives in the private sector are essential parts of teaching a new generation of users to be safe online.

4. Law Enforcement Assistance

The first and most important way to stop child pornography is to prosecute those who exploit children. Google takes seriously its responsibility to work closely with law enforcement to combat child exploitation. Google responds to thousands of law enforcement requests for assistance each year, and has a legal team devoted solely to this effort. We believe that we respond to hundreds of subpoenas a year as part of our cooperation in local, federal and international child safety investigations.

Google also regularly preserves data upon receipt from law enforcement officials of a data preservation request that is compliant with the U.S. Electronic Communications Privacy Act. Section 2703(f) of ECPA allows any government entity to require service providers to preserve records for up to 90 days, renewable for another 90 days with a mere request. Google preserves data in response to several hundred such requests a year.

5. Conclusion

Google keenly understands that our business relies on the existence of a healthy and trusted Internet ecosystem. Child pornography, and those who purvey it, should have no place in that system. For that reason, and as described in this testimony, we work on many fronts to combat this sinister activity: by cooperating with law enforcement, by supporting educational and industry efforts to keep kids safe, and by constantly working to improve our own technologies to the same end.

Thank you again for your leadership on this important issue. We look forward to working with you to protect all of our children on the Internet.

MR. WHITFIELD. Thank you.

And we appreciate the testimony of all of you.

And before we begin with questions, we do want to take time. Diana DeGette brought this issue up about what is going on in Great Britain with the Virtual Global Task Force. And there is a public service announcement in Great Britain that makes children more aware of how

they can report to law enforcement officials things that are going on on the cyber. And I think this would be informative for all of us, because really, we don't have anything quite like it in the United States. So if you all are prepared, I would like to show this video. It is about 2½ minutes, I believe.

MS. DEGETTE. Mr. Chairman, if I may, they apparently show this at movie theaters in Great Britain, and so I think I would say to all of the media representatives here today, this is exactly the kind of thing we need to do on your websites, on television outlets, and in movie theaters.

And I thank you for doing this.

[Video.]

MR. WHITFIELD. Okay. The first question I want to ask, it is not about AOL, but it is about the Internet service providers. There was some testimony, I think Mr. Lewis mentioned the policy on retaining IP addresses. And in all of the hearings that we have held on this subject from law enforcement, there was a lot of emphasis placed on that. And I know that some of the Internet service providers recently met with representatives of the Justice Department to talk about this issue.

So I would like to just start off by asking AOL and EarthLink and Verizon and Comcast. I guess Comcast has already answered, but what is the policy on retention of IP addresses at EarthLink, for example?

MR. BAKER. Mr. Chairman, our policy is, again, that we keep them in a live database for several months and then we archive them in tape backup, and our policy is now that we will keep those for 7 years. That is not to say they go back 7 years from today, but they are kept.

MR. WHITFIELD. And so what is the difference in live and in storage as far as the time that it would take to find that address?

MR. BAKER. Well, if I can just give you an anecdote. Just this last November, we got a subpoena from law enforcement for IP addresses, some of which were more than several months old, more than 5 months old, so these were in tape backup, and we were able to pull the necessary backup from archives, retrieve this information, and respond to law enforcement within 2 weeks, and this was notwithstanding Thanksgiving being during that period of time. So I would say that, in the case of tape backup, it might take a couple of weeks. Generally speaking, if it is of more recent vintage, we should be able to respond more quickly.

MR. WHITFIELD. And could you say about how many subpoenas you may receive in a month or a year?

MR. BAKER. We get about 1,000 subpoenas a year, so roughly 80 to 100 a month--

MR. WHITFIELD. Okay.

MR. BAKER. --from various law enforcement agencies.



MR. WHITFIELD. Okay, and Mr. Ryan, what is the policy for AOL?

MR. RYAN. The current policy, Mr. Chairman, with respect to retention of IP addresses is a 90-day period. We receive, at AOL, over 1,400 subpoenas a month, and that does not include search warrants, intercept orders, or other types of legal process on the criminal side. So it is over 14,000 subpoenas a year. It is a reflection of the size of our subscriber base.

MR. WHITFIELD. Right.

MR. RYAN. Recognizing that the 90-day period varies from, say, at EarthLink, we have a 24/7 dedicated staff for law enforcement only to make their requests for data, and we handled over 1,800 preservation requests last year. So we have a history of utilizing preservation with law enforcement, and the feedback that we get, with the current retention standards, coupled with our dedicated personnel, it works.

MR. WHITFIELD. Okay. And what about Verizon?

MR. DAILEY. Mr. Chairman, Verizon's policy for the data that we capture, and then we are talking about IP session logs, basically, that would link a customer or a user to a particular IP address, which I believe is what you are referring to. Our policy is 9 months.

MR. WHITFIELD. Nine months.

And how expensive is it to retain this kind of information? Is it a real factor to consider?

MR. RYAN. With respect to AOL, there is a cost factor. I think it is important to note that there are different kinds of IP addresses. There is a type of address we refer to as a proxy address, and that reflects the billion of sessions that go on on one particular day at AOL. An IP address is assigned to each one of those billion-plus sessions, so the retention period is far shorter, reflecting the volume. We did a cost study for the Department of Justice. To retain that information for up to 1 year would cost over \$44 million.

MR. WHITFIELD. \$44 million?

MR. RYAN. Yes, sir.

MR. WHITFIELD. Wow. And what about, Mr. Reiting, from Microsoft?

MR. REITINGER. Thank you, Chairman.

Of course, we are not typically a broadband provider--

MR. WHITFIELD. Right.

MR. REITINGER. --so we don't, in that sense, assign IP addresses to end users. The period of time we would retain data associated with a service could vary from service to service. I would be much more comfortable in addressing that in closed session, if the committee wants to do that.

MR. WHITFIELD. Okay.

MR. REITINGER. But what we try to do is balance law enforcement needs, business needs, and the privacy and security needs of our customers.

MR. WHITFIELD. Okay. I am really glad that this panel is here today, because as we told you in the beginning, we have had three or four sessions of hearings on this issue. And you think about the multitude of young people around the world who are certainly on the Internet today, being the wonderful tool that it is. Then we have the pedophiles out there and people who are trying to exploit them, and you all represent companies that provide them with the connection to the world, and you have such an important role to play. And actually our staff went on the Internet, and they put in "pre-teen" plus "sex" plus "video." And it was kind of interesting the different results that came back. For example, on Google, it came back with about one and a half pages, it is up there, and some of the language was so explicit, it has been redacted. And if you just look at the Google site, I mean, it looks like a hard core pornography site. I mean, sex games, and pre-teen sex, and teen porn, and triple-X movies with pictures and so forth. But I guess the most disturbing thing about on the Google site, Ms. Wong, and I know that you may not be involved in the policy, but you even had sponsored links. And what that means is you had people there paying Google money to advertise these kinds of sites on Google that young people have access to and everyone else. And I know the testimony of all of you today focused on your concern, and you want to protect children and you want to minimize the opportunity for them to be exposed to things like that. And I know that Google has a reputation of being a socially-responsible company. And I know that they recently hired a man, and I think his last name is Brilliant, to manage their foundation that is working with societal problems, disease, and climate issues and so forth. But to think that a company like this would be taking money from groups like this is sort of disturbing.

And I will give you a chance to respond, but before I do, we used the same words on the Yahoo! search, and it came up with five or six sites, but it was not nearly as sexually explicit. It is like "Dr. Phil on alarming sexual behavior among children," and "pre-teen healthcare," and "Fox News: Teen Sex and Media Hype," but there were no sponsored links. They were not receiving any money.

So I would like to just ask, what is responsible for the difference in what you receive on the search. And are you still taking money from people who are advertising this kind of material on the Internet?

MS. WONG. Thank you, Mr. Chairman.

And we actually greatly appreciated you and the committee staff raising this for us. We have no interest in getting advertising for the promotion of any illegal content or these types of ads. And in fact, we

think that this particular search was an aberration that was due to the fact that what the search was was “pre-teen.” If you were actually to search on Google for “preteen sex video” or “child sex video” or “young teen sex video,” ads would not show up at all. So what we did was we went back through our systems. We have a long list of black lists, and we have added the “pre-teen” to it, and no ads currently show.

But we do greatly appreciate the committee staff bringing it to our attention, and that is our policy: as soon as we become aware of it, we will either add it to a black list or remove it from the site.

In regard to our ads policy, and again, in conversation with the staff, we have actually tightened our policies to prohibit any type of ad that refers to teens in any way, including ads that may, in fact, have legal pornography on it but actually refer to teens.

MR. WHITFIELD. Okay. Well, what would account for what shows up as the result of the search using the same words with Yahoo! that we used with Google? The results were startlingly different, and the language used was unbelievably different.

MS. WONG. And I can’t really speak so much to how Yahoo!’s system works. We are many, many billions of pages. We believe we are probably about three times the size of any other search engine. So we have many more pages to screen and review. We do, as I was mentioning, have a many multi-tiered system for trying to remove these as soon as we find them, including getting lists, like from the Internet Watch Foundation, and there is also a similar organization in Germany, and immediately put those into place to block on our site. And we have our own search quality engineers who are trained to look for and remove these types of sites. We do the best we can.

MR. WHITFIELD. Okay. But it is the policy of Google now not to accept paid advertisement from groups like this?

MS. WONG. That is absolutely true.

MR. WHITFIELD. Okay.

Now Ms. Banker, you are with Yahoo!, aren’t you?

MS. BANKER. Yes, I am.

MR. WHITFIELD. Did you want to make any comment about any of this?

MS. BANKER. I would just note that Yahoo! strives to have an open and inclusive and comprehensive search product. Child pornography has no place in it, and for that reason, we use a number of techniques to identify and remove child pornography from our search index, including technical approaches, such as algorithms, reports from our users. It also reports from third-party sources, such as the IWF, to remove that content and report it to NCMEC as appropriate.

MR. WHITFIELD. Yes. So you are quite proactive on this issue, it sounds like.

MS. BANKER. Yes, we think that is appropriate, given the nature of the subject.

MR. WHITFIELD. Okay. Okay.

Now my time has expired. And in fact, I have gone over. And we have a vote on the floor. We have three votes. So I think we will take a break right now. Hopefully they can get this video fixed. Maybe you all could have a drink or a sandwich or something, and then we will come back. We will be back, I would say, in about 20 minutes. So we will recess for 20 minutes.

[Recess.]

MR. WHITFIELD. The hearing will come back to order.

I apologize for that delay.

I understand that we now are in a position to show this Virtual Global Task Force public service announcement, so if you would start it and run it for us, we would appreciate it.

[Video.]

MR. WHITFIELD. Thank you very much for getting that prepared for us.

And at this time, I will recognize Ms. DeGette.

MS. DEGETTE. Thank you very much, Mr. Chairman.

I think we could show that, don't you? Ms. Wong?

MS. WONG. I thought that was a very impressive PSA, and I actually would be pleased to discuss with your staff ways that we could work with it.

MS. DEGETTE. And they customize that for every region that they show it in in every country, so I think it is effective.

I want to thank all of you for coming and for your efforts to make the Internet safer.

The thing I want to say first, because I think we are getting a little confused about exactly what we are talking about here, and I think we need to know. There are really a number of interrelated issues. One of them is the solicitation of minors over the Internet through chat rooms and other mediums for sex and other activities. And I think all of you are making some very important voluntary efforts towards parental controls and technology plus parents talking to their kids and so on that goes to that.

The second issue is controlling child pornography over the Internet, which is an illegal activity, and which we need to take law enforcement methods to stop it. And there are a lot of issues around the first, chat rooms and so on, that I think we can explore. But I want to talk for a few minutes about that second issue, about how you all can assist law

enforcement in what is admittedly illegal activity that is happening over the Internet.

Let me start with you, Mr. Dailey, because you have had a broad regulatory authority. You would agree that nobody who is putting illegal information over the Internet would have any protection under contractual agreement with the Internet service providers, correct?

MR. DAILEY. I would expect that is very true for any ISP that I can think of.

MS. DEGETTE. Right. And I think nobody here would disagree. All of your contracts say that if you are doing something illegal over the Internet, we are going to report that to the authorities. So no one has a privacy interest in illegal activity over the Internet, right?

MR. DAILEY. I would agree with that. If there is any activity like that, it would be reported.

MS. DEGETTE. Right. Now Mr. Lewis, I wanted to, first of all, thank you very much for Comcast's announcement today that it is going to retain the customer-identifying data for 180 days. How much do you anticipate that it will cost Comcast to retain that data?

MR. LEWIS. I don't have an exact figure. I can certainly get it, but when we looked at the issue in light of recent discussions at the Justice Department, with this committee and staff members, and among ourselves and with other companies here and trade associations, we decided the investment was well worth it.

MS. DEGETTE. Yes. I would wonder, Mr. Chairman, if I could ask unanimous consent to have Mr. Lewis supplement his response within 10 days to let us know how much that will cost.

And Mr. Ryan, you stated unequivocally that your company is opposed to having to retain that type of data for a 1-year period, is that correct?

MR. RYAN. We are not opposing any discussion what are the best strategies. We are open. We are engaged in that discussion. In response to the question what the costs would be, we had prepared that, because the European Union requested that when they went through data retention.

MS. DEGETTE. And in fact, just so all of you know this, I am about to introduce legislation which would require all ISPs to retain customer identification data for a 1-year period. But the EU standards are even broader than that, correct? And they have adopted those standards, correct?

MR. RYAN. And each country now has to implement within their respective jurisdiction to what extent they are going to adopt that. That is correct.

MS. DEGETTE. Right.

MR. RYAN. And that was stage one.

MS. DEGETTE. Right. And I know your business and all of the other businesses here operate in international communities, so everybody is going to have to retain data for some period of time, correct?

MR. RYAN. That is correct.

MS. DEGETTE. Now Mr. Baker, your company retains the data for 7 years, correct?

MR. BAKER. That is our current policy.

MS. DEGETTE. How long has that been your policy?

MR. BAKER. Well, it depends which data we are referring to.

MS. DEGETTE. The customer identification data that we were talking about.

MR. BAKER. Right, customer billing address, initial dates of service, things like that--

MS. DEGETTE. Yes.

MR. BAKER. --which is sort of, if you will--

MS. DEGETTE. How long has that been your policy?

MR. BAKER. I will get you the exact date when that went into place, but it has been our policy for some time.

MS. DEGETTE. Some period of time. And how much does it cost you to retain those records?

MR. BAKER. I don't have figures on that.

MS. DEGETTE. Again, Mr. Chairman, I would ask that Mr. Baker be allowed to supplement.

MR. BAKER. I would be happy to provide this to you.

MS. DEGETTE. Ms. Banker, what about your company?

MS. BANKER. As mentioned in Microsoft's response on this issue earlier, companies like Yahoo! and Microsoft are in a slightly different position than some of the other companies--

MS. DEGETTE. That is right.

MS. BANKER. --so we would look forward to working with your staff to get clarity on how something like a data retention proposal might apply to a company that is primarily an online service.

MS. DEGETTE. That is right.

Mr. Lewis, I wanted to ask you, what caused your company to decide to retain the data for 180 days?

MR. LEWIS. Well, a variety of things, Congresswoman DeGette. In recent discussions, as part of the Department of Justice's working group, kicked off by the Attorney General and the FBI Director at the end of last month we became aware of the fact that our retention policy was on the shorter side compared to many other larger broadband commercial ISPs. We also, as I alluded to in my testimony earlier, had significant technical

problems last year that unfortunately impeded investigations. We are not proud of that.

MS. DEGETTE. Right.

MR. LEWIS. And we regret that. Those factors, combined with changed circumstances on the Internet, in particular the new aggressiveness and brazenness that we have seen demonstrated here today of predators, new forums for them to make their contacts and their connections, said to us that it was time to look at the policy carefully and revise it in light of our customer privacy obligations and commitments and in light of our privacy policies. And so that is why we made the decision.

MS. DEGETTE. And in fact, I will ask you, Mr. Dailey, there is no clear industry standard as to how long ISPs retain this type of data, is there?

MR. DAILEY. That is correct.

MS. DEGETTE. And it varies anywhere from 31 days, which I think was Comcast's previous policy, up to 7 years, is that correct?

MR. DAILEY. That is what I have heard today.

MS. DEGETTE. And I mean, all of you have expressed great grave concern for the safety of our children and for the desire to eliminate child pornography on the Internet. But the reason why we think it is important for ISPs to retain, not the communications, because the communications, those can be reported to different authorities, but to retain the identifying data so that during the course of law enforcement investigations, administrative or judicial subpoenas can be issued so that law enforcement officers can track down these perpetrators. Does that make sense to you, Mr. Lewis?

MR. LEWIS. Yes, it does.

MS. DEGETTE. Okay.

MR. LEWIS. I mean, our experience has been that we actively support law enforcement in these investigations, and have continuously since we--

MS. DEGETTE. Well, I know that, and I mean, the case that we have been talking about before today was the case where they found out about the child who was being raped on the Internet, and they went to Colorado and Comcast had destroyed the records, and I am sure that just makes all of your employees around the country feel sick. And it certainly was not intentional on Comcast's part.

MR. LEWIS. Well, that is, of course, right.

MS. DEGETTE. Yes.

MR. LEWIS. I mean, no one feels that more acutely than I do. I am a parent of two small children, myself, and what is depicted in that video, as I understand it, is horrifying. The company is not proud of the

technical problems we had last year. And the company has decided, in light of recent discussions with DOJ and others, to update and support law enforcement investigations with respect to child exploitation. Our commitment today is to extend our period to 180 days. Hopefully that goes a long way toward eliminating incidents like we had in Colorado last year. And that is our commitment.

MS. DEGETTE. And I hope you are willing to keep working with me and my staff so that we can get a standard to the industry.

MR. LEWIS. We are.

MS. DEGETTE. Just one last question, Mr. Lewis.

MR. LEWIS. Yes.

MS. DEGETTE. You said that your company favors giving NCMEC subpoena power, correct?

MR. LEWIS. Yes.

MS. DEGETTE. Now are you aware that NCMEC is not a governmental agency?

MR. LEWIS. We are, and there is certainly--

MS. DEGETTE. Do you know of any precedent where we gave a non-governmental agency subpoena power?

MR. LEWIS. I certainly don't off hand, but we could certainly investigate that if that is valuable.

MS. DEGETTE. Yes, I don't think that that happened. And furthermore, if they did subpoena records, I don't think they could be used in a criminal investigation, so I think it is creative thinking, but I don't think it would work.

Thank you, Mr. Chairman.

MR. WHITFIELD. Yes.

And at this time, I would recognize Mr. Stupak.

MR. STUPAK. Thank you, Mr. Chairman.

I apologize to the witnesses. I had to run out and speak, and unfortunately, at 2 o'clock, I have got to go speak again.

But earlier in my questions, I talked about going online here and putting in "pre-teen," "sex," and "video," and I have Google, I have Yahoo!, and I have MSN searches there. So let me ask a couple of questions, if I can, along this. It looks like Google is the most lenient. On this, when you take a look at it, the first says up here, not only do you have the websites, but you also have the sponsor links, so everyone else will have a sponsor link. Do you have that up, sponsor links up?

MS. WONG. No, and actually once it came to our attention from your committee's staff, we made sure that it was removed immediately. The problem appears to have been, we have a black list for key words that includes "preteen sex video" but without the hyphen. As soon as we



added the hyphen to the list, those no longer show. And in fact, we have added a number of others, thousands of other key words to that list.

MR. STUPAK. Okay. Ms. Wong, why do you put on here for adults only? Is there any way to enforce that?

MS. WONG. So what we have is a safe search filter, which a user can turn on to ensure that there is only the strictest level or the moderate level or no filter on their search.

MR. STUPAK. But wouldn't this cause more curiosity and cause more people to go to your site when you put things like "adults only" on it?

MS. WONG. Well, I think, for some children it could. We definitely believe, as Chris Hansen had mentioned earlier today, that this should be done with the parents' involvement, that the children should be having a range of issues to protect them, which include putting the computer in the living room.

MR. STUPAK. So other than taking off the sponsor links, have you done anything else to try to block this? Because Yahoo! has probably got about the best where they actually don't use the same type of wording, less suggestive wording, and you can't get in to see the videos and all of that. But yours was about the easiest site to access. And I guess my curiosity is why do we have different levels here of the ISPs? I would think you would all want to be on the same page.

MS. WONG. Well, from a search engine perspective, as opposed to the IP level, I think we all have different algorithms for identifying and including things in your index that accounts, in part, for why you may see different results.

MR. STUPAK. Right. And since you have different algorithms, if you are dealing with sex and pornography on your Net, couldn't you have more scrambling in that aspect and keep the rest of your search engine easy to access?

MS. WONG. Well, we have the safe phish filter, which makes it more difficult to access any sort of adult content.

MR. STUPAK. But obviously it is not working, because we were--

MS. WONG. And in addition, we have multiple layers to review. It is terrible that these sites are there, and we should--

MR. STUPAK. Well, I think we all agree, but it looks like your company is doing the least to try to block it or to stop it. That is, I guess, what I am trying to get at.

MS. WONG. Yes, and I think, in addition to the levels of review that we try to do to take it out, including getting third-party lists and that sort of thing and having our trained teams to try and find it, we also have the biggest search engine on the Internet. We have many billions of pages.

MR. STUPAK. So it is easier to find it. It should be easier to find it, so I would think you would have more filters and more ways to block it than the others if you have the biggest search engine.

MS. WONG. We have the biggest search engine. There are many more pages to review. And we are doing the best we can to identify as many of the illegal sites as we can and remove them as soon as we find them.

MR. STUPAK. Well, we have had discussions about this consortium that has recently been developed and AOL has sort of been leading that consortium. And the group invited Google to be part of it. And it says here in the article that was printed today you have not yet decided to do so.

MS. WONG. We absolutely think that that proposal is very promising. We were contacted last week to discuss it, and we are actively talking with them about it. We think there are a lot of things that we would like to work with them on, and we are actually just sort of flushing out exactly what the proposed work would be.

MR. STUPAK. Well, who is going to make the decision whether or not you join this group? I would think if you are the biggest and have the most, you would want to be part of the group instead of trying to go outside the group so you could learn what others are doing to block some of these sites.

MS. WONG. In terms of who has the ultimate decision, that is one that I will be making along with all of my executives. And in addition--

MR. STUPAK. Do you anticipate making that decision soon?

MS. WONG. Yes, we do.

MR. STUPAK. Okay. When?

MS. WONG. I know that the discussion happened over the weekend, and I am hoping that we have a decision this week.

MR. STUPAK. Okay. Let me ask Ms. Wong. In 1998, Congress actually passed a law where Internet providers were to contact the National Center for Missing and Exploited Children and having search engines do some work on that. Were you ever contacted by the Justice Department on that law, Section 13-032?

MS. WONG. I believe this is the law that has been challenged in the court and the Department of Justice is involved in litigation regarding it. We did receive a subpoena from them, it was a civil subpoena, seeking information from our company.

MR. STUPAK. Okay. When did that occur?

MS. WONG. That was last summer, I believe in August.

MR. STUPAK. Okay. Prior to receiving that subpoena, did you have any discussions with Justice on that proposed law?

MS. WONG. No.

MR. STUPAK. So the first you knew of it was the subpoena?

MS. WONG. We were aware of the law.

MR. STUPAK. Right.

MS. WONG. But the subpoena was our first involvement in their litigation.

MR. STUPAK. Okay. Anyone else care to comment on that? Section 13-032, Congress passed a law in 1998 directing Justice to take an active role in this, other than the subpoena, anyone else have any discussions with Justice about the law, whether they felt it was valid or what could be done and not done? Any of the others?

The reason why I ask, Congress passed the law in 1998. Justice came here about a month ago and said, "We think the law is faulty." And so I am trying to see if they ever did any research to see if it really was faulty or if this is just their way of suddenly doing something because we asked them to come back in 8 years later since they have done nothing for 8 years. By your silence, I take it Justice never contacted anybody.

Okay. Let me ask this question, if I can, Ms. Banker. In your testimony, you mentioned how Yahoo! trains law enforcement in child exploitation issues. Please explain the different types of training programs Yahoo! provides to law enforcement.

MS. BANKER. We have a number of programs in place. We focus a lot of our efforts in working with the Internet Crimes Against Children Task Forces, which, as I am sure you know, do a huge number of investigations when Yahoo! and other service providers provide tips to NCMEC. It is often the ICACs that follow up on those. We have been going around the country to the regional ICAC conferences and participate in the national ICAC conference on a yearly basis. We also provide sponsorship for these conferences. In addition to that, we reach out to other law enforcement agencies working for organizations, such as the National Association of Attorneys General. We also have been providing specific training for child exploitation prosecutors through the American Prosecutors Research Institute.

MR. STUPAK. I asked Ms. Wong a number of questions about Google there, and I indicated Yahoo!, I felt at least, had one of the better, different results, much more protected results. Can you just explain the difference between what you do at Yahoo!, how you block these sites?

MS. BANKER. We can certainly explain how we approach the issue. While Yahoo! strives to have an open and inclusive search product, child pornography is contraband, and it has no place in our index. And for that reason, we use several techniques to try and eliminate it from the search product. We use algorithmic approaches to identify it. We also use user reports. And then we use outside agencies, such as the IWF, which

provides a list of sites that we then remove from our search index. Once we have removed sites, we then report them to the National Center for Missing and Exploited Children.

MR. STUPAK. Okay. Mr. Ryan.

MR. RYAN. Yes.

MR. STUPAK. Mr. Ryan, we had talked, or I had mentioned earlier, about Great Britain and how they had, like 18 percent of all of the websites on pornography, and now it is down to 0.4 percent. And you were in the lead, along with, I think, Yahoo! was the other who worked on that. It worked in Great Britain. Can it work in this country? Are there barriers to what you did in Great Britain that would prevent us from cracking down here in the United States?

MR. RYAN. Well, what works in Great Britain and what we contribute to it is when the IWF does their research and locates sites that contain child pornography, they distribute that to companies, including our AOL operation in the UK. And we have agreed, to the extent that we have the capability to block access to those sites, we do that. And we do that on a daily basis. The complexity is probably the most direct answer why efforts in the United States have not been as successful. That is not to say when we are put on notice or we learn on our own about potential sites, we will, and have, blocked access to those sites.

MR. STUPAK. Where is the problem? Is it NCMEC not getting the information to you? I know part of it. The ISPs, there are only like 215 who will voluntarily work with NCMEC while there are about 3,000 or more. What is the breakdown here? I guess that is what I am trying to--

MR. RYAN. Well, there is no entity. NCMEC is not proactively searching the Internet for sites that contain child pornography. They are the recipient of reports.

MR. STUPAK. Correct.

MR. RYAN. They are not proactive. They rely on law enforcement or other entities, such as the IWF, to do the reporting for them. So I mean, I think you are leading towards, I think, a good suggestion, an entity like the National Center. If they could be given the resources to conduct similar research, I think that is a great avenue to pursue.

MR. STUPAK. Well, Great Britain, I read somewhere that, I think, Microsoft gave them like \$4 million or something to help establish this center. Is that right, Mr. Reitingner? Oh, that was the Canadians. You gave the Canadians \$4 million, right? Was that to establish a center to be proactive to report these sites to monitor it, to get them shut down like they did in Great Britain? Was that the reason for it or--

MR. REITINGER. Ranking Member, I am not sure precisely what you are referring to. We have worked with the Canadian law enforcement

officials in several matters. I think you might be referring to our work to develop CETS, the Child Exploitation Tracking System.

MR. STUPAK. Right.

MR. REITINGER. We have committed over \$5 million to the development and deployment of that system, which is an open standards-based tool that can be deployed by law enforcement anywhere to cooperate and track child pornographers, child exploiters, and work together--

MR. STUPAK. But what you are doing in Canada, would that work here?

MR. REITINGER. Yes.

MR. STUPAK. Okay.

I am sorry, Mr. Chairman.

MR. WHITFIELD. Mr. Pickering.

MR. PICKERING. Thank you, Mr. Chairman, and thank you for your series of hearings on this very important matter.

Ms. Wong, help me just to understand what the status is currently with Google's cooperation with providing the DOJ with the information that they requested under COPA.

MS. WONG. We have fully complied with the request, as narrowed by the Federal judge in San Jose.

MR. PICKERING. Now, as I understand it, AOL, Yahoo!, and Microsoft complied voluntarily and completely from the very beginning, but Google did not and took it to court. Is that correct?

MS. WONG. That is correct.

MR. PICKERING. Now in your earlier statement, you said child exploitation and child pornography is horrific and vicious. And what I am trying to understand is over time, the policy of Google and the culture of Google, is it to view child exploitation and child pornography as horrific and vicious, do everything you can to cooperate with DOJ and with law enforcement and to not have sites that were pulled up earlier when you type in "pre-teen" plus "sex" plus "video." And I think you probably have seen all of those sites that came up and would agree that many of them are completely unacceptable. I guess what I am trying to understand, has Google, through this process of hearings and through the enhanced scrutiny of what is happening on the Internet and the danger to children, have you all come to a clear position both legally and culturally within your corporation or your policies to be more cooperative and more vigilant?

MS. WONG. Just to be very clear, we were in long discussions with the Department of Justice over that civil subpoena and to also explain our process, we comply with criminal subpoenas and all law requests on a daily basis. And in fact, we prioritize requests that have to do with child

safety. We are seeking to do a turnaround for them in terms of our response within 24 hours, if not within a few hours of getting that response. The civil subpoena from the Department of Justice was not directly related to child pornography. It was a request for our entire search index, billions of URLs in our index and millions of search queries that were, as I understand from the consultant to the Government, intended to create a model of the Web, generally to test their theory on whether software filtering was actually working.

MR. PICKERING. But why was that possible for all of the other companies at the table but not possible for Google? And does it show a cultural difference and a marketing and a business difference between the companies? Do you want to be known as the company where teenagers can have access to teen pornography and where your clients can go into child pornographic sites feeling like they will be protected and their information will not be given to the Government?

MS. WONG. Certainly not. We, in no case want to be a safe haven for child pornographers or anyone engaged in illegal activity. And I couldn't speak to it. My other colleagues did in terms of their response to the Government and how much they ultimately produced to the Government. In our case, we worked with the Government for several months to try and give them information that would be helpful to them and ultimately weren't able to reach an agreement and then to go to the judge.

MR. PICKERING. Now as I understand it, too, when the committee staff brought this to your attention as to what is available on Google's sites, you changed your sponsorship policy, and you corrected your protective mechanism to include a hyphen when added so that these types of sites would not be pulled up, is that correct?

MS. WONG. That is right. We enhanced the blocking list, which had several hundred keywords to block on it. We apparently missed the hyphen in "pre-teen," and we have now added that and actually thousands of others.

MR. PICKERING. And I realize that you all's search engine is much larger than most of the other industry companies, but there is at least an appearance that Google is not being as cooperative or as vigilant on these issues. And the question is, is there a desire by Google to be free of all? And as you know, there are some people that take a position that constitutionally, everything goes: child pornography, child exploitation, even bestiality; all of those things should be accessible and should be constitutionally protected. And I guess what I am trying to understand, do you have a corporate culture that leans toward that philosophical view? And do you want to have a business plan with that philosophy? Or do you, as you testified, view it as horrific and vicious and that you

need to be vigilant in both your corporate policy, your legal policy, and to stop having your search engine pull up these types of things and have sponsorships on it? It seems like the committee hearings and the oversight has created a change in policy. But what we want to know is, is this a real change or is this simply for public relations during a time of scrutiny?

MS. WONG. Congressman, our entire company feels very deeply that we want no part of child pornography, or any obscenity that is illegal. We also, from our executives on down, are deeply committed to this in our actions and principles. In fact, my CEO, Eric Schmidt, was recently speaking in Europe and personally committed to the endeavor to remove all of this from our search engine and any of our services.

MR. PICKERING. Well, let me, one, commend you for changing your policies and correcting and protecting. But let me also tell you, we will be watching very closely, and we want all of the companies to be good actors. We don't want any bad actors in this industry and for the Internet. We will, as a committee, and I think you can see, be very vigilant and will not rest until we have the right assurances and policies and, if necessary, legislation to more effectively protect our children.

So thank you, Ms. Wong.

MS. WONG. Thank you.

MR. PICKERING. Mr. Chairman, I yield back.

MR. WHITFIELD. Thank you, Mr. Pickering.

We are going to have another quick round here, and I understand there may be another member or two coming. But we are getting close to the end here.

I would like to ask Mr. Baker, one of the first hearings we had, we had a young man named Justin Berry that received a lot of publicity around the country. And he was very brave to come in and talk about how he became involved in this whole child molestation issue. And he ended up meeting people at rendezvous locations and so forth. But he mentioned the fact that he really became involved in this, not that there is one issue that did it, but he did say that he received a free webcam from EarthLink that was given as an incentive to sign up. And I was just curious, do you all still give away webcams for encouraging people to sign up? Not that there is anything wrong with it, but I was just curious if you do.

MR. BAKER. No, Mr. Chairman. We have not distributed webcams since 2002.

MR. WHITFIELD. Okay. Okay.

And Mr. Ryan, I know one of the measures that you all take, and I guess you mentioned this a little bit earlier, to find and shut down illegal activity involves hashing of images and monitoring of chat rooms. And

it is my understanding that your company is the only one that has the hashing technology? Or is that correct or not?

MR. RYAN. I can't speak with certainty about that. In fact, since the Coalition has been formed, a couple of my colleagues, some of them here today, have illustrated they do have some tools available that they are utilizing that work within their network. And that speaks to the potential benefit of the Coalition, to bring all of those resources together, share what works and may work in other network environments. So I am optimistic that my colleagues are doing something and that collectively we can do more.

MR. WHITFIELD. So every company at the panel today is represented in that task force?

MR. RYAN. Not everyone, but certainly the invitation extends to everyone, and we will have a dialogue with everyone.

MR. WHITFIELD. Which companies do belong to that task force?

MR. RYAN. EarthLink, Yahoo!, and Microsoft.

MR. WHITFIELD. Okay. Okay. Would you just elaborate a little bit on hashing, the way that works?

MR. RYAN. The way it works in our environment is every time a file is uploaded or downloaded, when I say "file," I mean the attachment to an e-mail transmission, we work with the National Center. They have identified referred files that they believe, by their expertise, to contain child pornography. Each file contains a unique signature. And we populate a database at AOL with those signatures associated with files that have been identified by NCMEC as containing child pornography. Any time a file is attempted to be transmitted through our network, it is matched against that populated database. If it contains a signature that has been identified with child pornography, we remove that, we package it, and we refer that to the National Center for investigation.

MR. WHITFIELD. Now I am not sure that you all are responsible for what goes on in Europe with your companies, but, from your understanding, how would you measure the effectiveness that we are having with this problem in the United States as compared to, say, the European Union?

MR. RYAN. Well, I could speak with some authority with that, because we work closely with our colleagues in the UK with this project. Because it is one common network, the AOL UK operation is actually using the AOL network here in the United States, here in Virginia. When the IWF makes a request to the AOL UK to block a site, that request actually comes to us here in the United States and technicians that work under, my direction implement that block. So that block is not only effective for access or attempted access by UK subscribers but also the entire AOL subscriber base.



MR. WHITFIELD. Yes.

Would anyone else want to address the European Union issue?

Okay. All right. Oh, let me have one other question here.

Mr. Lewis, in responding to Diana DeGette's questions, you talked about some of the technical problems that prevented Comcast from tracing IP addresses for some law enforcement subpoenas or whatever.

MR. LEWIS. Yes.

MR. WHITFIELD. What efforts did Comcast make to remedy that problem? And from your perspective, has that problem been solved?

MR. LEWIS. Yes, I am happy to report that the problem has been solved, and we believe our systems are working fully in supporting all of our legal and law enforcement practices as well as our own internal practice. The problems are very technical and complicated, having to do with rolling out what is called a provisioning system, the software and hardware that issues accounts to customers, lets us add new customers quickly, and lets them get service quickly so they could use what they purchased from us. It became apparent slowly over time last year, in particular to the legal response center team that handles law enforcement requests, that we may be having a problem. They went back and did independent investigation with the technology teams that have built this system and, in the early summer, determined that there were problems. We acted quickly to mobilize the technical teams to address the problems. We had weekly conference calls with senior vice presidents and myself to emphasize the importance of these fixes and to make them quickly. And at the same time, the legal response center instituted a series of manual processes so that we could support as many legal and law enforcement requests as we could while we worked to fix the system. That process continued throughout the fall of last year and early into this year. The new fixes, if you will, for the software system were ready at the beginning of this year. They were tested, tested again, and rolled into production this spring. And as I said, the problem is now remedied. We took it very seriously. The problems impacted not only our support for law enforcement, which of course was a primary concern, but our ability to run and manage other aspects of our business. We had every incentive in the world to make these fixes quickly and efficiently, and we worked as hard as we could to make them. And we believe now the problems are behind us.

MR. WHITFIELD. Thank you, Mr. Lewis.

I recognize Mr. Stupak.

MR. STUPAK. Thank you, Mr. Chairman.

Mr. Reiting, the Financial Coalition Against Child Pornography, which you are part of, was supposed to bring together Internet industry leaders, leading banks, credit card companies, third-party payment

companies, and Internet service companies, including Microsoft. And you are joined with the National Center for Missing and Exploited Children in the fight against child pornography. Our information tells us that pornography on the Internet is a \$21 billion industry where downloading music is about a \$3 billion industry. It is seven times greater. Can you explain what is happening there? And I would really be interested to see what are the credit card companies and the third-party payment companies doing? Because it seems like as long as I have a credit card, I can buy anything on the Internet with any name, with any address, with any location. So how would you crack down on this Internet sale?

MR. REITINGER. Thank you, Ranking Member.

The credit card companies, and I don't want to do too much speaking for them, because we are not a credit card company, and they face challenges, because it can be hard to determine what a merchant is doing or not doing.

MR. STUPAK. Sure.

MR. REITINGER. Like the Internet companies, they have no interest in supporting child pornography. Everyone wants to expunge child pornography from their systems. And so this is a joint effort for companies, like the financial services companies, some key Internet companies, and the National Center to figure out and share best practices and mechanisms to expunge the use of those systems, those credit card payment systems from supporting the distribution of child pornography.

As a former law enforcer, I can tell you this is sort of a tried and true technique. One of the classic ways to go after crime is to go after the money pieces, the old--

MR. STUPAK. Absolutely. I mean, on this committee, in the 10 years I have sat on it, 12 years, we have done things like we have had cats actually buy Viagra over the Internet. As long as we had a credit card, we could buy anything we want. And with this pornography, it seems the same way, or to drug masking agents that we have had hearings on earlier this year. I agree with you. If we go after the money, we could dry up part of this, but we just can't seem to get anywhere. So I was wondering if you were looking at that aspect and if you had any suggestions we could make today. Or would you let us know if you move along in that direction? Because if you get the money, I think we can, not completely, but at least cut down on this. I mean, with seven times greater than downloading music, it is pretty disturbing.

MR. REITINGER. Thank you, sir.

I don't have any specific suggestions to offer today. I would like to go back and check with people in our company that are more specifically involved in that.

MR. STUPAK. Okay.

MR. REITINGER. But clearly, in terms of investigation, as you suggest, following the money is a great way to go to really bring these people to justice.

MR. STUPAK. Mr. Chairman, I think one more thing we should do is to get credit card companies and the third-party payment companies--I really think we should get them in and see what they are doing on this issue, much like we have had the ISPs here.

MR. WHITFIELD. We are planning to do that.

MR. STUPAK. Good.

Whoever wants to answer this, maybe go down the line. I have a couple quick questions here, if I can.

Do you all support requiring ISPs to keep parent-child pornography reports to make to the National Center for Missing and Exploited Children for at least a 90-day period, even before a preservation order is made? Mr. Ryan?

MR. RYAN. Yes, that is the proposal that we are submitting today and are prepared to do on a voluntary basis.

MR. STUPAK. Okay.

Mr. Baker?

MR. BAKER. We would be prepared to do so as well.

MR. STUPAK. Okay.

Ms. Banker?

MS. BANKER. Yahoo! actually already maintains a significant amount of that information, and we would be happy to look at a proposal to make sure we conform.

MR. STUPAK. Okay.

Mr. Dailey?

MR. DAILEY. Verizon would be willing to do that as well.

MR. STUPAK. Okay.

Mr. Lewis?

MR. LEWIS. Comcast would be willing as well, sir.

MR. STUPAK. Mr. Reitinger?

MR. REITINGER. We do that, sir.

MR. STUPAK. Ms. Wong?

MS. WONG. We would be prepared to do it.

MR. STUPAK. Okay. Then would you all support giving NCMEC the preservation order authority so that NCMEC can directly request the ISPs keep the child pornography image, IP address, and other information which would cut down on the time it takes for local law enforcement to be able to get the preservation order?

Mr. Ryan?

MR. RYAN. Yes, AOL supports that.

MR. STUPAK. Okay.

MR. BAKER. Yes.

MR. STUPAK. Ms. Banker?

MS. BANKER. Yes, we support that.

MR. STUPAK. Mr. Dailey?

MR. DAILEY. Verizon does as well.

MR. LEWIS. Comcast as well, sir.

MR. REITINGER. Yes, sir.

MS. WONG. Yes, we would support it.

MR. STUPAK. Okay. We are going pretty good. How about one more?

Do you all support following the voluntary submitting guidelines that AOL and other ISPs developed with NCMEC to report child pornography? DOJ has never issued the rules that the 1998 law is talking about, so some of the ISPs took the initiative to develop their own rules, and DOJ has refused to allow the ISPs, who have created the guidelines, to send it to other ISPs. That is why we only have 215 ISPs who have registered with NCMEC. So would you support voluntarily submitting the guidelines that AOL and the others have developed for this purpose?

MR. RYAN. Yes, AOL supports that.

MR. STUPAK. Mr. Baker?

MR. BAKER. Yes, I believe so.

MS. BANKER. Yes, Yahoo! supports that.

MR. STUPAK. Okay.

MR. DAILEY. Verizon supports that with one comment or caveat, and this is something I reported in my testimony. It is the issue of a clarification under 13-032 that when an ISP submits an image along with their report to NCMEC that that would be clarified and indicate that it is not a distribution of child pornography. So we think that that is a useful clarification--

MR. STUPAK. Right.

MR. DAILEY. --to the extent any ISP is not reporting images at that point, and we think that would be helpful.

MR. STUPAK. I know the DOJ has got some problem with that, which we are still trying to understand up here.

MR. DAILEY. But other than that, we do support it.

MR. STUPAK. All right. Okay.

Mr. Lewis?

MR. LEWIS. Yes; with the clarification that has been mentioned, we would support that, sir.

MR. STUPAK. Okay. Mr. Reitingner?

MR. REITINGER. Yes, sir; we support that.

MR. STUPAK. Ms. Wong?

MS. WONG. Yes.

MR. STUPAK. Okay. Do you all support including location information along with the ISP address to NCMEC?

MR. RYAN. Yes. In fact, AOL initiated it.

MR. STUPAK. You do, at any rate?

Mr. Baker?

MR. BAKER. Yes.

MS. BANKER. We currently comply with that practice.

MR. STUPAK. Okay.

MR. DAILEY. Yes, in general for Verizon Online, we would support that notion. It is a question of availability and appropriateness, depending on the type of report. Since we are dealing sometimes with spam, e-mails, things like that that we send in, I am not sure it always applies, but when it applies, we certainly would provide that.

MR. STUPAK. Okay.

Mr. Lewis?

MR. LEWIS. Yes, if the information is available to us, we would support that.

MR. STUPAK. Okay.

MR. REITINGER. Yes, sir; if available.

MS. WONG. Yes.

MR. STUPAK. One more question.

Do you all support requiring the ISPs to take proactive steps to block child pornography from traveling on your network?

Mr. Ryan, I know you are already doing this.

MR. RYAN. Yes, we are committed to that.

MR. STUPAK. Correct.

MR. BAKER. Yes.

MR. STUPAK. Ms. Banker?

MS. BANKER. Yes, we currently take proactive measures to locate child pornography.

MR. STUPAK. Okay.

MR. DAILEY. Verizon has not actually joined the technology group that has been pulled together.

MR. STUPAK. Right.

MR. DAILEY. But we do support the notion of using technology, and we will support investigations into that.

MR. STUPAK. Okay.

MR. LEWIS. We would do so likewise.

MR. REITINGER. Sir, we already filter images uploaded to groups and spaces.

MR. STUPAK. Okay.

Ms. Wong?

MS. WONG. We are joining the others in looking at those new technologies.

MR. STUPAK. Okay. Thank you. I wish all of the questions were that easy.

Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you.

At this time, I will recognize the full committee Chairman, Mr. Barton of Texas.

CHAIRMAN BARTON. Thank you, Mr. Chairman.

I apologize for not being in here for the hearing in its entirety. I have got about five different things I have been working on today, and I just wasn't able to be here.

But this is one of the highest priority issues before, not only this subcommittee, but this full committee. And if we have a good hearing tomorrow, which I am expecting that we will, it is my intention to touch base with our leadership on the Minority side, and, based on the hearing record, see if we can't develop very quickly a comprehensive anti-child pornography piece of legislation. This is a serious, serious issue, and the parents of America, and I think the Congress, is tired of just talking about it. I think we are ready to take fairly drastic and definitive action in a comprehensive way to really put a damper on child pornography in this country. So I am thankful for this panel of witnesses.

I really only have one generic question. And Mr. Stupak was asking some very good specific questions, but my generic question is if we can prove that an Internet site is engaged in child pornography or transmitting images that have child pornography in them, why is it not possible to immediately terminate that site? That is my generic question. I mean, you have to be able to have some agency of the Government, I guess, definitively say, "That is child pornography." But once that is established, why can't we just immediately cut off that site so that nobody else can get to it?

MR. RYAN. John Ryan from AOL, sir.

Certainly once we have noticed that a site is hosting child pornography, we can take measures to block access on behalf of our members who may seek access to that site. If your question, though, is to terminate that site, that action must be directed to the host of that site. And many times AOL is rarely the host of that type of site but merely a dumb conduit to that site. So blocking access is one measure. Terminating that site, in your language, is another measure.

CHAIRMAN BARTON. I am not computer-literate, so, in laymen's terms, what I am getting at is the brief in here talks about hotline tips and stuff, about 1,500 a week are able to be determined that they are

exhibiting, exposing, transmitting child pornography. What I would like to see, and I am willing to put it into law, if it is necessary, that once you have established not waiting for a court to go out and convict the people that are operating the site, but just immediately, if termination is the wrong thing, deny access so that nobody can get to it. I mean, just put in the law if a specific site is determined that it does have child pornography content, as soon as that is established, boom, nobody gets to it. And even if they have these dynamic IP addresses, it would have to help if you can't go back to the site. Yes, sir.

MR. REITINGER. Thank you, Chairman.

I think I can say for probably everyone on the panel that if on one of our properties, for example a space or a group or an individual website someone uploads child pornography, the moment we discover that, either through an external report or through our own filtering mechanisms, we immediately, and I can certainly speak for us, take that site down.

CHAIRMAN BARTON. You do that today?

MR. REITINGER. Yes. And we report the matter to NCMEC, the National Center for Missing and Exploited Children.

CHAIRMAN BARTON. Well, that is my only question, if nobody else wishes to answer. I just am very concerned about this, and I would assume that all of our witnesses support whatever steps are necessary to lessen this scourge. And there is not any civilized society in the world where child pornography is legal. And it is certainly not legal in the United States, so whatever we need to do in the Internet age to really go after it, I am totally for.

I would be happy to yield to Mr. Stupak.

MR. STUPAK. Yes, Mr. Chairman, if you would.

The last question that you asked, do you take down the site immediately, Mr. Reiting, you said you do, AOL does. Do the rest of you? Because it is my understanding that not all of you do that.

Mr. Baker?

MR. BAKER. No, if it is a site we host, we would take it down immediately.

MR. STUPAK. Okay.

Ms. Banker?

MS. BANKER. Any time we detect child pornography, we do remove that content from our site immediately.

MR. STUPAK. Okay.

MR. DAILEY. If it is on a Verizon server, we will remove it.

MR. STUPAK. Okay.

MR. LEWIS. And the same for us. If it is within our control, we will remove it and report it to NCMEC.

MR. STUPAK. Okay.

Ms. Wong?

MS. WONG. Yes, as soon as we are aware of it.

MR. STUPAK. Okay.

Thank you, Mr. Chairman.

CHAIRMAN BARTON. And I want to thank Mr. Stearns for letting me go out of order.

And I yield back, Mr. Chairman.

MR. WHITFIELD. Thank you, Mr. Chairman.

At this time, I will recognize Mr. Stearns.

MR. STEARNS. Thank you, Mr. Chairman.

Let me ask each of you. How many of you have chat rooms? I am going to be a little elementary here. Just raise your hand if you have a chat room.

Okay. So you are putting your hand this way. Why are you not giving a yes or no for a chat room? Just if you don't mind, move the mic a little closer to you.

MR. REITINGER. I am not fully up to speed on this, sir, but we used to have chat rooms, and I think we still do, but only as part of a subscription service.

MR. STEARNS. So if a person subscribes to a Microsoft system service, they would have a chat room?

MR. REITINGER. There are specific services you could subscribe to where a chat room would be available. Yes.

MR. STEARNS. Would be available. Okay.

Within these chat rooms, I guess to the three of you then, can you outline what safeguards you have in these chat rooms? It is pretty elementary.

Go ahead, Mr. Ryan. Why don't you start?

MR. RYAN. Yes, sir. First of all, with the Kids Online service, which is for minors only, those are completely monitored. Every chat room that is made available and the parents enable their minor to access those chat rooms, then they are monitored in real time by AOL staff who are empowered. In fact, the written testimony has pointed out, we receive training from experts at the National Center to look out for warning signs for potential, what was referred to earlier as, "grooming" of these minors in an effort to either send them a contact--

MR. STEARNS. So let us say we have, what, five people, ten people? How many people do you have?

MR. RYAN. Oh, no. There are hundreds.

MR. STEARNS. Hundreds of people who are monitoring this chat room. And let us say they find a grooming, then what happens?

MR. RYAN. It is reported immediately to the National Center for their review and investigation.



MR. STEARNS. And then the National Review Center, have they been cooperative with you? Have they responded?

MR. RYAN. Yes, this is the partnership that we entered into as a best business practice, and in fact, it has been responsible for over 153 arrests since the program was initiated approximately 2½ years ago.

MR. STEARNS. Okay.

Next, I think it is Ms. Banker. Would you say Yahoo! then--

MS. BANKER. Yes, Yahoo! does offer chat rooms to our users.

MR. STEARNS. And do you have safeguards?

MS. BANKER. We do have safeguards in place. First of all, our chat service is restricted to users are registered with us as being 18 or older. We also have built-in safety content as part of our chat service and include a report abuse link as part of every chat window. So whenever a user is in using the chat room, if they see something inappropriate, they can immediately click that link. We have built special tools to enable user reporting that is particularly useful for our customer care service when they are reviewing reports and allow any reports that would indicate activity involving solicitation of a minor or illegal content that we can escalate those reports immediately and report them to the National Center for Missing and Exploited Children. We have also been engaged in a dialogue with the National Center and the Internet Crimes Against Children Task Forces about how we might further improve our chat product.

MR. STEARNS. Anything that you might want to add?

MR. REITINGER. Yes, sir, and I apologize because, again, I am not fully aware of all of the details of the chat, but our chat services are, to the best of my knowledge, only available as a part of subscription service. So there will be financial information associated with that, which makes things more traceable. We also provide general education to users about Internet safety and safe use of services and also have abuse reporting mechanisms available in case there is abuse.

MR. STEARNS. I chair a subcommittee. We dealt with videogames, and the question came up, the folks who were making the software and the ratings system were saying that a person has to be over 17 to purchase this game. Well, we showed that you go on the Wal-Mart site, and they say, "Are you over 17?" And the person could just check off "yes." So Ms. Banker, how can you corroborate that they are any age group or not? Like you said that you make sure it is only a certain age group. I mean, how do you confirm that?

MS. BANKER. At the point of registration, Yahoo! asks users to provide their date of birth so that we have an age available in our system. Our terms of service require that they provide true and accurate information. And I agree with you that it is a very difficult problem

around verifying that age. We certainly looked into whether there are systems available that we could implement that would allow us to continue to offer the robust array of free services that we currently have. And we have not been able to identify a technology that is really available that would allow us to do that at this point.

MR. STEARNS. Yes.

Now when you are trying to monitor these chat sites and you feel that you have all of these people, do you believe that we, as Federal legislators, could have additional authority to allow you to be more proactive searching and eradicating, for example, if you find something and you want to retain it on your hard disk or you want to keep a file of this, you might be a little bit nervous to keeping all of this in your library here, because you might be accused of what you are trying to eradicate. So I guess the question is do you think anything legislatively needs to be done to allow safeguards to protect you in your eradication process and your proactive activities?

This could be anybody, if they want. It is an open-ended question if anybody feels that there is some legislative fix that would be helpful for you. If not, I mean, just say no.

MR. DAILEY. In the context of NCMEC reporting, as I mentioned earlier, we have indicated in our testimony, this is Tom Dailey speaking from Verizon, that we would like to see some protection built into 13-032 so that as we are reporting images to NCMEC along with our reports in the CyberTipline that we would not find ourselves also being accused of disseminating pornography when we are trying to report it.

MR. STEARNS. Well, that is why I asked the question.

MR. DAILEY. Thank you.

MR. STEARNS. Okay. So maybe Mr. Dailey, my last question is directed to Verizon. You might want to just establish for the record. The staff has indicated to me that Verizon was unable to make reports using the CyberTipline in January through March of this year. I guess the question is why, or you might just want to elaborate on that.

MR. DAILEY. Yes, thank you very much for the opportunity to do so.

There was a period of time at the beginning of this year for roughly 3 months where we were having a combination of things, really. We were having a transition from one organization to another, of security personnel. Essentially, the people actually have to do the work, transitioning from one employee who left to another. And then there was a reorganization. And unfortunately, that left us, frankly, not able to report, anything that had come into our inbox, into our security box. So it was really an administrative problem on our part that was corrected. And once we got ourselves reestablished with our security organization, there was a brief period of time where we had some technical issues in

terms of hooking into the CyberTipline that caused some delay, but it was really an organizational problem on our end. And once we were able to get that individual back in place, reviewing the abuse logs, he did go back and try and find those that had built up over time and report them. In all of the cases, though, that we have reported since then, approximately 116 at last count, none of them were images. They were all falling into the general category that I referred to earlier as what I would call child pornography spam. These are e-mails that people sent to us saying that they had received them. We sort of broadened our scope of what we thought was reportable, and we forwarded them on. So these are not cases where people were reporting active solicitations or predation or even images.

MR. STEARNS. Did you make reports to the NCMEC through another channel?

MR. DAILEY. At this time, no.

MR. STEARNS. Okay. Okay.

Mr. Chairman, that is all of the questions that I have. Thanks.

MR. WHITFIELD. Thank you, Mr. Stearns.

At this time, I will recognize Mr. Walden if he has any additional questions.

MR. WALDEN. Thank you, Mr. Chairman.

Mr. Lewis, is it currently possible to have 100-percent response rate, that is in response to every law enforcement request Comcast could identify a subscriber?

MR. LEWIS. That would certainly be the goal. That is what we strive for. The reality is that the systems that support our over 9 million customers and growing every day are extraordinarily complex and are dispersed throughout the country where we serve our customers. It is always our goal. We are not satisfied with less than 100 percent. The reality of working with large, complicated hardware and software systems is there is always a small failure rate. We are working to minimize that as much as possible.

MR. WALDEN. Sure.

Is Comcast trying to develop a system or a program that would allow them to fix those instances where they cannot identify a subscriber?

MR. LEWIS. Well, as I mentioned earlier, we corrected the problems that we had last year and into early this year. Those problems are now fixed, and as far as we are aware, there are no remaining issues. We are actively monitoring the network. The Legal Response Center team that handles these requests periodically tests the system with sample data and throws hundreds of thousands of queries at it and analyzes the results by hand to make sure that the data coming back is accurate and verifiable. Our primary goal in supporting legal and law enforcement requests is not

only to provide a prompt response, it is to provide an accurate response, because no one's interests are served, law enforcement's, the companies', or certainly customers', with inaccurate responses. So we are actively monitoring the system. We believe it works well. We are currently testing it, and in conjunction with the rollout for the 180 days that we announced earlier, we will be doing further testing to verify the integrity and accuracy of that system.

MR. WALDEN. I want to follow up on that 180-days issue. In your testimony, you said that you support the concept of data preservation with regard to informations relative to NCMEC for those sorts of referrals. Does Comcast do that already?

MR. LEWIS. We do, to the extent that we run into reportable events over NCMEC. The nature of our business is somewhat different from some of the other companies here today. We don't provide extensive features for customers to meet or congregate, such as chat rooms, nor do we provide widely used features for customers to upload or make content available publicly. We primarily provide a premium, high-speed Internet connection with e-mail accounts that people use however they see fit. Where we run into reportable NCMEC events in the overwhelming majority of cases is actually through our interaction with customers typically in their homes. A standard scenario would be a Comcast service technician would go to a home to install cable modem service or to repair a problem and as the first panel and Mr. Hansen's video demonstrate, many of the people involved in this activity are quite brazen. A technician will go to the customer's computer, turn it on, and see what appear to be child exploitation or pornography images on the computer. They may observe magazines or other photographs on a coffee table. And in cases, the customer may approach the technician and ask him or her if they are interested in seeing more pictures like this. It is horrifying and amazing. And understandably, our technicians want to get out of there as quickly as possible. And our policy and procedure is for them to report these incidents immediately to their supervisors who are, in turn, instructed to report them to the legal department. I will field many of the requests personally. We will interview the technician, and we will make a determination whether it is reportable to NCMEC or not. We made several reports ever since we have operated our service since early 2002, and I can assure you that we err on the side of reporting if there is any doubt.

MR. WALDEN. Thank you.

Mr. Reiting, why did the number of reports that you sent to the CyberTipline increase in the past year? Was this due to a filtering device that Microsoft uses?

MR. REITINGER. Sir, I think the stats for the last year actually went down slightly.

MR. WALDEN. Really?

MR. REITINGER. But my information was between the year before and last year they went down slightly. And I don't know the causality for that.

MR. WALDEN. Okay. But do you use some sort of filtering device now that--

MR. REITINGER. We do use a filtering device. We use a proprietary algorithm that scans images when they are uploaded to spaces or groups. And if they are flagged as pornography, then they are reviewed. And if it constitutes reportable child pornography, we make a report to NCMEC.

MR. WALDEN. But did the filtering itself increase reports to NCMEC? Did that help?

MR. REITINGER. I would have to get back to you on that. I am not personally aware of the correlation, but I know there has been some discussion about that.

MR. WALDEN. Okay. You would think it would. But I mean, I would appreciate knowing that.

And this is a question to all of the companies. Is there anything legislatively that you believe you would require in order to do more to eradicate child pornography from your networks? I know in earlier testimony, I don't remember if it was Mr. Ryan or Mr. Baker who made the comment about a concern of transmitting data to law enforcement, could you potentially be prosecuted because you are transmitting child pornography, in effect, as part of giving the law enforcement a tip. Aside from something like that, what needs to be done legislatively? What would you recommend?

MR. RYAN. Well, that is not a concern of AOL. We believe--

MR. WALDEN. Right.

MR. RYAN. --the current reporting statute authorizes us, in fact mandates us, to forward that to the National Center if, in fact, that is part of the report that we receive.

MR. WALDEN. Right.

MR. RYAN. I would just echo some of the comments that were made earlier with respect to when we are more proactive, when we were not operating under statutory guidelines but we do want to do more proactive searching and filtering, that we enjoy the protections of immunity during the processing of that information if it does contain potential images that are illicit, that we are covered and protected in these.

MR. WALDEN. So you believe you are covered?

MR. RYAN. Under the existing statute.

MR. WALDEN. All right.

Mr. Baker? Was it you who raised that issue?

MR. BAKER. I think it was Mr. Dailey who raised the point, and I will let him speak for himself.

MR. WALDEN. Okay.

MR. BAKER. But to the extent that there is legislation, let me put it this way, if it is not already clear that the investigation of a child pornography complaint is not possession and that the transmittal of such a complaint to NCMEC is not transmission, then it should be made clear.

MR. WALDEN. Okay. But beyond that though, go ahead.

MR. BAKER. And if I may just go a step further, regarding the technology alliance that several of us have announced, it is another additional benefit of that in that we will not actually be transmitting images but rather just the digital signatures that are assigned to certain images. So that does add another layer of protection as well.

MR. WALDEN. All right.

Ms. Banker?

MS. BANKER. I would just add to those comments that one of the key things that we really think could be done legislatively is to give the National Center for Missing and Exploited Children the ability to issue preservation requests when they receive tips from the CyberTipline so that they can immediately contact ISPs who may have information related to those tips and have them preserve data.

MR. WALDEN. And I want to hear from the others in the 2 minutes I have, but I also want to throw one other thing up because we heard this in prior testimony at a prior hearing, and that was from kids who said one of the most damaging things they have is the notion that as a child, in some cases, their sexual images were put up on the Internet. Is there ever a way to scan and retrieve and destroy those? Or are they out there for life? And I just throw that out, because that was a real troubling feature, I think, for everybody. Something that may have been done to them as an infant could be on the Internet forever. Is there a way to technologically scan and destroy?

MS. BANKER. I don't know if there is a way technologically today to do that, but a number of us are going to be working together as part of a Technology Coalition, and we will be looking at a number of different issues. And I think that is certainly a very important and valid issue to add to the agenda.

MR. WALDEN. It would seem to me if you could search for different things, you might be able to search for a known image, identify it, and then somehow destroy it. I don't know. I don't know how you all make ones and twos do what you do.

Anyway, Mr. Dailey?

MR. DAILEY. Actually, Mr. Baker is correct. It was I that raised the point about assuring that reports to NCMEC would not be considered distribution of child pornography, and the problem is that there does appear to be some ambiguity, at least in our opinion, in terms of the distribution laws under Section 22-52(a). So our thinking was a clarification in the NCMEC statute 13-032 would be relatively simple to make and would help eliminate any ambiguity.

MR. WALDEN. Right.

MR. DAILEY. And beyond that, I would second Ms. Banker's comments about adding preservation authority to NCMEC.

MR. WALDEN. All right.

MR. LEWIS. From the Comcast perspective, sir, to the extent there are any technical discrepancies or ambiguities in the reporting statute, clearly we support closing those. Another legislative option I would ask the committee to consider would be increased funding and support for law enforcement. In the close relationships we have with many law enforcement agencies, they often are forced to choose and make difficult decisions about cases to pursue or not based on their available resources. We have provided and would be willing to provide additional forensic and other training and support to help them do their job better to work with us, and I think resources for law enforcement as well as training and expertise from the private sector would help significantly.

MR. WALDEN. Okay. With regard to this NCMEC issue and the right to subpoena and all, have you discussed that with NCMEC? What is their response, if you have? And I am way over my time.

MR. RYAN. Yes, I can address it. I actually serve as the chairman of the Law Enforcement Committee as a board member at the National Center.

MR. WALDEN. Right.

MR. RYAN. And there was a proposal submitted to the full board that was approved 2 weeks ago endorsing the notion of getting legislative authority for preservation requests for the National Center.

MR. WALDEN. All right. All right.

Mr. Reiting, Ms. Wong, if you want to--

MR. REITINGER. I will just briefly echo Mr. Lewis' comments. As a former, again, law enforcer, it is my view that no child predator or exploitation or pornography case should go unprosecuted for want of resources.

MR. WALDEN. Good for you.

MR. REITINGER. It is just too critical an area. And the training and forensic difficulties and pure agent time can be disabling for Federal law enforcement.

MR. WALDEN. All right.

Ms. Wong?

MR. REITINGER. That is it.

MS. WONG. We would echo the calls for preservation ability for NCMEC, because that seems to handle a lot of the issues that law enforcement is having. In addition, we have been working with WiredSafety to develop materials that train local community police officers to go into schools and train the children and putting together materials and software for them. And I think legislation that would fund that type of education across the board for parents, police officers, and kids would do a great deal, as Chris Hansen's testimony earlier spoke of.

MR. WALDEN. All right. Thank you very much.

MR. DAILEY. May I add one more point to that? This is just a personal service announcement, but I think the notion of getting into the curriculum in our schools, our elementary schools, education on cybersecurity is every bit as important as many of the other things that are there. As the parent of two kids, as I mentioned at the outset, both of whom have gone through the Fairfax County schools, neither one of them got any cyber education up through the fifth or sixth grade. I think there are some changes maybe afoot in Fairfax County, but I think that is something that ought to be mandatory for all kids.

MR. WALDEN. Perhaps it should be mandatory for all parents of all kids, too.

MR. DAILEY. I would agree with that, too.

MR. WALDEN. Thank you.

Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you, Mr. Walden. And I want to thank all of you for being with us today. I am sure it has been an enjoyable day for you. You have been here a few hours, and--

MR. STUPAK. Mr. Chairman, before they all leave we have talked a lot, but we never got to peer-to-peer, a little bit of this material, and when we talk about images, we have to find a way to block the peer-to-peer from person to person, and whether it is Comcast, Verizon, or AT&T, we have to be able to take that. So when you are meeting on your 21<sup>st</sup> Coalition, or whatever they call it there, I hope they take that aspect into it. That is a whole other part of this hearing. We could go on for an hour just on the peer-to-peer stuff. And Mr. Walden talked about the pictures. Those are some of the things we are concerned about. How do you stop the peer-to-peer? So I would be interested in some suggestions like that.

MR. WHITFIELD. Absolutely.

And as you heard, Mr. Barton talked about some legislation, so I am sure that you will be hearing more from Mr. Barton and his staff and the committee staff about that.



And without objection, we will move all of these documents into the record, include them formally into the record. And certainly, we will keep the record open for 30 days. And then tomorrow, we will continue this hearing.

But you all are dismissed at this time. And thank you, again, for your cooperation and expertise.

Thank you.

[Whereupon, at 2:57 p.m., the subcommittee was adjourned.]

## **MAKING THE INTERNET SAFE FOR KIDS: THE ROLE OF ISP'S AND SOCIAL NETWORKING SITES**

---

**WEDNESDAY, JUNE 28, 2006**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ENERGY AND COMMERCE,  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 2:05 p.m., in Room 2123 of the Rayburn House Office Building, Hon. Ed Whitfield (Chairman) presiding.

Members present: Representatives Whitfield, Walden, Burgess, Blackburn, Barton (ex officio), Stupak, DeGette, Inslee, and Dingell (ex officio).

Staff present: Mark Paoletta, Chief Counsel for Oversight and Investigations; Alan Slobodin, Deputy Chief Counsel for Oversight and Investigation; Karen Christian, Counsel; Kelly Andrews, Counsel; John Halliwell, Policy Coordinator, Mike Abraham, Legislative Clerk; Ryan Ambrose, Legislative Clerk; David Nelson, Minority Investigator.

MR. WHITFIELD. I would like to call this hearing to order and I certainly want to welcome everyone today. Today we hold the second day of hearings on making the Internet safe for children, the role of Internet service providers and social networking sites.

Yesterday we heard from the Internet service provider community about what they are doing to eradicate child pornography from their networks and to facilitate law enforcement's ability to investigate and prosecute those predators and purveyors of child pornography. I was pleased to learn about the new initiative of AOL, Yahoo!, Microsoft, Earthlink, and United Online announced yesterday which brings the technological expertise of these companies together for the sole purpose of coming up with proactive solutions to purge their networks of child pornography.

Today we will hear testimony about the social networking sites for children and teens. Unlike the Internet, social networking sites have grown in popularity among children and teenagers. As an example, in its testimony today, Fox Interactive Media, the parent company of MySpace.com, notes that it has approximately 250,000 new registered

users per day and there are currently 85 million members. We will also hear testimony from two other networking sites, and due to the fact that the social networking sites like MySpace, Xanga, and Facebook are free to register and there is no way to verify the age of the users, and adults certainly can access those sites and it is very difficult, at least it is my understanding, to determine what the age really is, that is an issue that we certainly want to focus on.

I look forward to hearing from each of the three sites today about their products and how they encourage safe social networking among their young users. I hope MySpace, Xanga, and Facebook, working with State and Federal law enforcement agencies, State attorney generals, Congress, the National Center for Missing and Exploited Children, and others can develop a gold standard to create a safe environment for children. We also look forward to the testimony today of representatives from the Federal Trade Commission and the FCC.

Finally, I want to thank Detective Dannahey from the Rocking Hill, Connecticut, Police Department for agreeing to testify on such short notice about his fascinating work on a social networking site and to educate the subcommittee members about how these sites could be used by child predators to endanger our children. I certainly want to also thank the attorney general from Connecticut for testifying at the hearing about his thoughts on enhancing safety for children on social networking sites.

[The prepared statement of Hon. Ed Whitfield follows:]

PREPARED STATEMENT OF THE HON. ED WHITFIELD, CHAIRMAN, SUBCOMMITTEE ON  
OVERSIGHT AND INVESTIGATIONS

TODAY WE HOLD THE SECOND DAY OF HEARINGS ON “MAKING THE INTERNET SAFE FOR KIDS: THE ROLE OF ISP’S AND SOCIAL NETWORKING SITES.” YESTERDAY WE HEARD FROM THE INTERNET SERVICE PROVIDER COMMUNITY ABOUT WHAT THEY ARE DOING TO ERADICATE CHILD PORNOGRAPHY FROM THEIR NETWORKS AND FACILITATE LAW ENFORCEMENTS ABILITY TO INVESTIGATE AND PROSECUTE THESE OFFENSES. I WAS PLEASED TO LEARN ABOUT THE NEW INITIATIVE AOL, YAHOO, MICROSOFT, EARTHLINK AND UNITED ONLINE ANNOUNCED YESTERDAY WHICH BRINGS THE TECHNOLOGICAL EXPERTISE OF THESE COMPANIES TOGETHER FOR THE SOLE PURPOSE OF COMING UP WITH PROACTIVE SOLUTIONS TO PURGE THEIR NETWORKS OF CHILD PORNOGRAPHY.

TODAY, WE WILL HEAR TESTIMONY ABOUT SOCIAL NETWORKING SITES FOR CHILDREN AND TEENS. UNLIKE THE INTERNET—SOCIAL NETWORKING SITES HAVE GROWN IN POPULARITY AMONG CHILDREN AND TEENAGERS. AS AN EXAMPLE, IN IT’S TESTIMONY TODAY, FOX INTERACTIVE MEDIA, THE PARENT COMPANY OF MYSPACE.COM NOTES THAT IT HAS APPROXIMATELY 250,000 NEW REGISTERED USERS PER DAY AND THERE ARE CURRENTLY 85 MILLION MEMBERS.

DUE TO THE FACT THAT SOCIAL NETWORKING SITES LIKE MYSPACE, XANGA AND FACEBOOK ARE FREE TO REGISTER, AND THERE IS NO WAY TO VERIFY THE AGE OF THE USER CHILDREN AND ADULTS CAN LIE ABOUT THEIR AGE. I LOOK FORWARD TO HEARING FROM EACH OF THE THREE SITES ABOUT THEIR PRODUCTS AND HOW THEY ENCOURAGE SAFE SOCIAL NETWORKING AMONG THEIR YOUNGER USERS. I HOPE IS THAT MY SPACE, XANGA, AND FACEBOOK WORK WITH STATE AND FEDERAL LAW ENFORCEMENT AGENCIES, STATE ATTORNEY GENERALS, CONGRESS, THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN AND OTHERS CAN DEVELOP "GOLD STANDARDS" TO CREATE A SAFE ENVIRONMENT FOR CHILDREN. WE ARE ALSO LOOKING FORWARD TO THE TESTIMONY OF THE FTC AND THE FCC.

FINALLY, I WOULD LIKE TO THANK DETECTIVE DANNAHEY FROM THE ROCKING HILL CONNECTICUT POLICE DEPARTMENT FOR AGREEING TO TESTIFY ON SUCH SHORT NOTICE ABOUT HIS FASCINATING WORK ON A SOCIAL NETWORKING SITE AND TO EDUCATE THE SUBCOMMITTEE MEMBERS ABOUT HOW THESE SITES COULD BE USED BY CHILD PREDATORS TO ENDANGER OUR CHILDREN. I WOULD ALSO LIKE TO THANK THE ATTORNEY GENERAL FROM CONNECTICUT FOR TESTIFYING AT THE HEARING ABOUT HIS THOUGHTS ON ENHANCING SAFETY FOR CHILDREN ON SOCIAL NETWORKING SITES.

MR. WHITFIELD. At this time, I would like to recognize the Ranking Member, Mr. Stupak of Michigan, for his opening statement.

MR. STUPAK. Thank you, Mr. Chairman, for continuing these hearings that are so vital to the safety of our children.

Yesterday, Chris Hansen of Dateline NBC showed us how pervasive the grooming of children by online predators is. He expressed concern about how pedophiles use social network sites including MySpace, Facebook, and Xanga. These websites have grown exponentially in a matter of months. Xanga has 29 million subscribers. MySpace is a little over 18 months old and already has 85 million subscribers, up from 30 million when Newscorp bought it last summer. These sites are also extraordinarily popular with children and adolescents. Twenty-two million of MySpace's members are underage. Clearly the social networking sites have developed a massive following.

However popular that they are, these sites cannot survive if they act as a fertile hunting ground for predators seeking children to exploit, use them, or worse. Whatever social need they fulfill, these websites cannot be allowed to serve as an unfretted avenue for pedophiles to stroll and troll, so how do we clean up these sites? The root of the problem is the inability or unwillingness of these networks to limit communications to age-appropriate groups. Chris Hansen told us yesterday that the predators they encountered were all over the age of 18. While I am sure that these social networking sites do provide opportunities for teens to prey sexually on other teens, it is adult pedophiles that we are concerned about. MySpace and its competitors do ask children their ages. Federal

law requires that they establish that their clientele is at least 13 years of age but too often these social networking sites use an honor system to determine the ages of children on their sites. Only recently after a flurry of bad publicity that is affecting their bottom line and their public image did these social networking sites appear willing to invest in cleaning up their networks. While these recent efforts are appreciated regardless of their motivation, much more must be done.

Each of these social networking sites must take aggressive and immediate measures to keep young kids off their systems, enact meaningful safeguards for teens, and seek out and block child predators from their systems. MySpace will describe various interim steps that they have taken to try and protect 14- and 15-year-olds while the company searches for the holy grail of the effective age-determining software. They will also try to discredit the “no one under 18” policy that for instance Yahoo! imposes on the use of its chat rooms by saying kids will just lie about their age. This argument misses the point. The point is that the pedophiles don’t shop the 18 and over crowd, they aim for the 22 million or so MySpace underage users. I believe MySpace wants nothing to do with pedophiles and is willing to spend the money to limit their access to MySpace. However, it is clear that the steps that MySpace and its competitors have taken thus far are woefully insufficient.

Every week another news article appears about another child harmed by a predator that found his victim on MySpace. When our staffs were given a tour of the FBI’s Innocent Images Control Center for Internet Child Abuse Crimes, an agent went online posing as a 13-year-old girl that liked soccer. No other information was provided. This fictitious 13-year-old drew six responses from men seeking inappropriate conversation within the 15 minutes that the staff observed the exercise. Chris Hansen told us yesterday that we may be wrong about the statistic that one in five children have been approached sexually online. He said a Dateline NBC commissioned study suggested the number was closer to one in three. Sites that encourage teens to reveal their personalities, likes and dislikes, and express their thoughts online will by their very nature attract predators.

With my law enforcement background, I understand the danger that these sites pose to our children if the status quo continues. Saying that nothing can be done to keep our children safe is no longer an option. One could argue that Congress should simply wait for the sites to implode because of the bad publicity or let the free market force these sites to act more responsibly, but the free market has failed to date and made online child pornography a multibillion dollar industry. Every day we wait for the companies to change, millions of children are left

vulnerable. I would suggest to the committee and to our witnesses that our patience is wearing thin. If we do not start seeing real change with real results, Congress will need to act swiftly to address this issue.

With that, Mr. Chairman, I yield back the balance of my time.

MR. WHITFIELD. Thank you very much. Mr. Walden, did you want to make an opening statement?

MR. WALDEN. No.

MR. WHITFIELD. At this time I recognize the gentleman from Michigan, our Ranking Member, Mr. Dingell, for an opening statement.

MR. DINGELL. Mr. Chairman, thank you for your courtesy. I wish to add my congratulations for an excellent series of hearings regarding the scourge of child pornography over the Internet. This is a dirty business as the hearings show. It is in need of substantial legislative correction. You, Representative Stupak, and the other members of the subcommittee have done a fine job of identifying many methods used by the pedophiles and predators who abuse our children for perverted fun and profit. You have also identified many of the weaknesses in our system that allow these unfortunate abuses to flourish.

Industry counterparts in the United Kingdom have volunteered to do their part. I am curious, why haven't ours and why can't they? In the United Kingdom, Internet service providers, ISPs, must take down every site identified as a child pornography site by national and international law enforcement within 48 hours of notification. Further, these Internet firms must block all users of their platforms from accessing identified child porn sites worldwide. Moreover, I note that if these companies also find an effective way to block identified images from being transferred over their networks, they could make a considerable dent in the for-profit business of supplying pictures and videos of children raped, defiled, and tortured. The Internet industry must also find more effective ways of cooperating with law enforcement and perhaps they should show a bit of desire to do so. Why can't data that links IP addresses to physical locations be stored longer and accessed on a much more timely basis in response to subpoenas from Federal, State, and local investigators? Why shouldn't all information relating to identified child porn sites be properly forwarded to law enforcement and stored for use in future prosecutions? There also needs to be continuing oversight of the Federal agencies that under current law are responsible for dealing with this problem. The Attorney General makes quite a point of the priorities this Administration places on catching and prosecuting these predators but does his department's child exploitation section share his sense of urgency? Where are the regulations necessary to ensure consistent and effective ISP reporting of offending images? Why are ISPs not required to register, resulting in less than 20 percent of these firms reporting any

child porn information to the National Center for Missing and Exploited Children? And there are serious questions whether the Federal Trade Commission and the Federal Communications Commission have the authority and the resources necessary to provide much oversight. Federal, State, and local enforcement agencies have done an excellent job given the fact that they have limited resources available. We must provide more funding, particularly for the interagency Internet Crimes Against Children Task Forces that are fighting an uphill battle against those who abuse our children. More funds need to be appropriated for forensic computer capability so that the prosecutions can proceed on a timely basis. We must act aggressively to address this epidemic of evil which threatens our children. Today's hearing, which will shed further light on these new social networking websites that have captivated so many of our children and provided such a fertile hunting ground for predators, is an important step.

I look forward to working with you, Mr. Chairman, and all of my colleagues to fight this scourge, and I will do everything I can to work with you and my colleagues to make this an effective undertaking.

I yield back the balance of my time.

[The prepared statement of Hon. John D. Dingell follows:]

PREPARED STATEMENT OF THE HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS  
FROM THE STATE OF MICHIGAN

Mr. Chairman, let me add my congratulations for an excellent series of hearings regarding the scourge of child pornography over the Internet. You, Rep. Stupak, and the other members of the Subcommittee have done a commendable job identifying the many methods used by the pedophiles and predators who abuse our children for perverted fun and profit. You have also identified many of the weaknesses in our system that allows this abuse to flourish.

Industry counterparts in the United Kingdom have volunteered to do their part – why can't ours? In the United Kingdom, Internet Service Providers (ISPs) must take down every site identified as child pornography by national and international law enforcement within 48 hours of notification. Further, these Internet firms must block all users of their platforms from accessing identified child porn sites worldwide.

Moreover, I note that if these technology companies also find an effective way to block identified images from being transferred over their networks, they could make a considerable dent in the for-profit business of supplying pictures and videos of raped, defiled, and tortured children.

The Internet industry must also find more effective ways of cooperating with law enforcement. Why can't data that links IP addresses to physical locations be stored longer and accessed on a much more timely basis in response to the subpoenas from Federal, State, and local investigators? Why shouldn't all information relating to identified child porn sites be promptly forwarded to law enforcement and stored for use in future prosecutions?

There also needs to be continuing oversight of the Federal agencies that under current law are responsible for dealing with this problem. The Attorney General makes quite a point of the priority this Administration places on catching and prosecuting these

predators. But does his Department's child exploitation section share his urgency? Where are the regulations necessary to ensure consistent and effective ISP reporting of offending images? Why are ISPs not even required to register, resulting in less than 20 percent of these firms reporting any child porn information to the National Center for Missing and Exploited Children? And there are serious questions whether the Federal Trade Commission and the Federal Communications Commission have the authority and resources necessary to provide much oversight.

Federal, State, and local law enforcement agencies have done an excellent job, given the limited resources available. We must provide more funding, particularly for the interagency Internet Crimes Against Children taskforces that are fighting the uphill battle against those who abuse children. More funds need to be appropriated for forensic computer capability so that prosecutions can proceed on a timely basis.

We must act aggressively to address this epidemic of evil that threatens our children. Today's hearing, which will shed further light on these new social networking Web sites that have captivated so many of our children and provided such a fertile hunting ground for predators, is an important step. I look forward to working with all my colleagues to fight this scourge.

MR. WHITFIELD. Thank you, Mr. Dingell. We appreciate your opening statement. Dr. Burgess, do you have an opening statement this afternoon?

MR. BURGESS. No.

MR. WHITFIELD. At this time, I will recognize Ms. DeGette of Colorado.

MS. DEGETTE. Thank you very much, Mr. Chairman, for another important hearing on how we can protect our children from the increasing use of the Internet by pedophiles and rapists.

Yesterday we talked mostly about the access provided by Internet service providers to those who commercialize these images and today of course we are going to continue the examination that began yesterday with Chris Hansen of Dateline NBC. Today we are going to talk about social networking groups, a relatively new Internet phenomenon where millions of kids and teens post personal information on the web to share with peers and to meet new friends. This may be a new phenomenon but it is a familiar one to me because I have two daughters, ages 12 and 16, who have used some of these websites and fortunately, as far as I know, have not been solicited for improper purposes, but the problem is, of course, predators are now flocking to these sites and using them for improper purposes. I am particularly pleased, Mr. Chairman, that you asked Detective Frank Dannahey of the Middletown, Connecticut, police force to testify today because like so many dedicated law enforcement officers, Detective Dannahey is in the trenches investigating the ways predators prey upon our children trying to track down as much of the problem as possible and so he can help us understand just how easy it is for pedophiles to infiltrate these websites where large groups of kids are



having dialogs and find out more about them than any private eye could have before the advent of companies like MySpace.

MySpace has received so much of this attention because it is the largest of these social networking sites. Estimates are that nearly 85 million users have established personal pages on their network over just the last 18 months and apparently there are 22 million minors who have pages on the site but Mr. Chairman, there is another number that should trouble us greatly. According to a news report, MySpace has only 54 million unique users. That leaves 31 million pages for duplicate postings, and I wonder how many of these 31 million users claim to be multiple ages.

One thing we do know and one thing I am interested hearing about in the testimony is that MySpace has no mechanism in place to identify the people who request postings on their network, much less to verify their ages. Yesterday we were told that Yahoo! limits its chat rooms to persons over the age of 18, and Microsoft requires payment for its forum, thus limiting its use to people who possess a credit card, which would in most cases be a demographic that skews older, but it is certainly not foolproof. I suspect that Yahoo!, MSN, and other sites who try to limit access only to adults are far less attractive hunting grounds for predators seeking sex with a child, but one thing I am interested in hearing from everybody from the detective on down is, how we can protect around minors and others who just get around these restrictions that people try to put in place. I myself saw my 12-year-old daughter do it by just--not on MySpace but on a different age-restricted website where she just typed in a different birthday and was able to pretend she was somebody older. We need to keep in mind, and I think actually Congressman Burgess mentioned this yesterday, Masha Allen, who was the 13-year-old who begged us to help her take down the images that were posted on the web by the man who adopted her and raped her from ages five to ten. Well, certainly that was not someone she met in the chat room. She stands as a plea for all of these teenagers and younger who are being abused over the Internet, and all of us need to work together--Congress, parents, police agencies, and the companies themselves, to stop the pedophiles from using what should be a tool to keep an open and honest way of communication and finding legitimate ways to have new friends for nefarious purposes.

So Mr. Chairman, I look forward to hearing the witnesses today and I yield back the balance of my time.

MR. WHITFIELD. Thank you, Ms. DeGette, and at this time I recognize the full committee Chairman Mr. Barton, who has been particularly supportive of our efforts in these series of hearings and recognize him for his opening statement.

CHAIRMAN BARTON. Thank you, Chairman Whitfield, for the fifth day of hearings on this continuing problem that we are trying to address.

Today we are going to hear from some of our law enforcement individuals and from some of the social workers and some of the websites that are designed especially for children and teenagers.

Yesterday we heard from the Internet service providers. They testified before this subcommittee and announced their plans to implement new initiatives or policies to make their networks safer for children. For example, one provider said that it would lengthen the time that it keeps its data. Another would no longer accept advertising from websites who claim to include sexual images of teenagers. The group of the providers including some of the largest in the country, AOL, Yahoo!, MSN, and Earthlink, announced the coalition to create the Center for Child Protection Technologies at the National Center for Missing and Exploited Children. This center is going to be dedicated to developing new technologies and law enforcement strategies to detect and prevent the transmission of child pornography over the Internet.

Today we are going to hear from social networking sites about what they are doing to keep their sites safe for children. These sites are something completely different than any experience most of us in this room have ever had when we were children. Facebook and MySpace are like high school yearbooks except that the world looks at them, and some of the people looking unfortunately are predators hunting for prey. Almost every day there is a new report describing an adult who was able to communicate with a child or teenager through a social networking site. Sometimes these contacts end in tragedy, a child being assaulted by an adult after meeting online. I want to know what the social networks are doing to ensure that predators are not able to exploit their websites to meet children.

I understand that some of the social networking sites who will testify before us today have recently strengthened their safeguards for children on their sites. I appreciate that these sites are devoting additional resources and attention to the issue. However, it is important that they continue to be vigilant so that they remain one step ahead of the predators who seek to use their sites to abuse children.

This isn't an academic exercise for me. I have a stepdaughter who is a junior in high school. She has a profile on one of these sites. Her mother has been very vigilant with her about communicating what she can and cannot put on her profile and who she can and cannot share it with in terms of giving certain specific information to. So I am very concerned not just as a legislator, but as a stepparent about the issue that is before us today.

There is no greater priority than the fight against child pornography and the sexual exploitation of children over the Internet. As I announced yesterday, at the conclusion of these hearings it is my intention to work with Mr. Dingell and others on the Minority side to craft a comprehensive anti-child pornography piece of legislation that will if necessary give additional tools to help win this fight. Again, as I said yesterday, I think the Congress is tired of talking about it and I think the parents of America are tired of talking about it. I think it is time for us to take responsible, reasoned action to protect our children against these despicable child predators that are on the loose right now in our land.

And with that, Mr. Chairman, I yield back.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY  
AND COMMERCE

Thank you, Chairman Whitfield, for convening this second day of hearings on the role of Internet Service Providers and social networking sites with regard to the sexual exploitation of children over the Internet.

Yesterday, some of the Internet Service Providers who testified before this subcommittee announced their plans to implement new initiatives or policies to make their networks safer for children. For example, one provider announced its intentions to increase its data retention period. Another provider confirmed that it will no longer accept advertising from websites who claim to include sexual images of teenagers. In addition, a group of providers, including AOL, Yahoo!, MSN, and Earthlink, announced that they will join together to create the Center for Child Protection Technologies at the National Center for Missing and Exploited Children. This center will be dedicated to developing new technologies and law enforcement strategies to detect and prevent the transmission of child pornography over the Internet.

Today, we will hear from social networking sites about what they are doing to keep their sites safe for children. Almost every day, there is a new report describing how an adult predator was able to contact and communicate with a child through a social networking site. Sometimes, these contacts end in tragedy, with the child being assaulted by an adult he or she met online.

I want to know what the social networks are doing to ensure that predators are not able to exploit their websites to meet children. I understand that some of the social networking sites who will testify before us today have recently strengthened their safeguards for children on their sites. I appreciate that these sites are devoting additional resources and attention to this issue. However, it is important that they continue to be vigilant so that they remain one step ahead of the predators who seek to use their sites to abuse children.

There is no greater priority than the fight against child pornography and the sexual exploitation of children over the Internet. As I announced yesterday, I intend to pursue comprehensive anti-child pornography legislation in order to help win this fight. For this reason, I look forward to hearing your thoughts and proposals on what can be done by law enforcement, by the industry, and by Congress to make the Internet safer for our children.

I look forward to hearing from the witnesses and yield back the balance of my time.

MR. WHITFIELD. Thank you, Mr. Barton.

At this time I recognize Mrs. Blackburn of Tennessee.

MRS. BLACKBURN. Mr. Chairman, I have no statement.

MR. WHITFIELD. Thank you. I think we have concluded all the opening statements so at this time I would like to call the witness on the first panel, Detective Frank Dannahey of the Rocky Hill Police Department from Rocky Hill, Connecticut, and Detective Dannahey, we appreciate your being with us today to share with us your experiences on this very important topic. As you know, in Oversight and Investigations, we like to take testimony under oath. I am assuming you have no difficulty doing that.

MR. DANNAHEY. No, not at all.

MR. WHITFIELD. And I am also assuming you do not have the need for legal counsel today.

MR. DANNAHEY. No, I don't.

MR. WHITFIELD. If you would raise your right hand.

[Witness sworn.]

MR. WHITFIELD. Thank you, very much, and you are under oath now and you are recognized for 5 minutes to give your opening statement, which we look forward to.

#### **STATEMENT OF FRANK DANNAHEY, DETECTIVE, ROCKY HILL POLICE DEPARTMENT**

MR. DANNAHEY. Thank you, Mr. Chairman.

Good afternoon, Chairman Whitfield, Ranking Member Stupak, and members of the subcommittee. I am Detective Frank Dannahey of the Rocky Hill, Connecticut, Police Department. I have been a member of law enforcement for the past 25 years. For the last 15 years I have been assigned to the youth division of the Rocky Hill, Connecticut, Police Department.

Over the last 7 years I have been involved in investigations and education concerning Internet crimes against children. I have served in an online undercover capacity to detect Internet predators. My current efforts involve safety programs directed towards parents, students, school officials, and law enforcement. In the past 7 years I have seen technology change in a direction that both benefits and assists online predators in carrying out their criminal activities. With the majority of America's teens online, the pool of potential victims is vast.

In February 2006, an incident occurred in Middletown, Connecticut, that attracted national attention. Seventeen females from the ages of 12 to 16 were victims of sexual assault by older males that they met on MySpace.com. All of these crimes occurred within a very short period

of time. I was asked by the Middletown Police Department to assist them with parent programs on Internet safety. As these programs for Middletown were being developed, we were contacted by Dateline NBC. Dateline was interested in profiling these crimes as well as reporting on the educational programs for parents.

While preparing for the educational programs, I became involved in an online test of teen vulnerability. In a departure from the normal type of online undercover scenario, I took on the role of a teen male named Matt. Matt was a 19-year-old new kid in town who was looking for online friends from Middletown, Connecticut. I was particularly surprised and shocked to see that a majority of young teens who were 14 and 15 years old allowed Matt onto their private page. The information on a private page is not viewable by anyone else unless that person allows someone on as a friend. Some teens questioned Matt about who he was before allowing him on their MySpace page as a friend. Many teens allowed him on as a friend with no questions asked. Once Matt was allowed on the teenagers' MySpace pages, it became immediately obvious that personal information was readily available and easily volunteered. I was able to find out such information as where a teen lived, worked, their full names, and date of birth, where they went to school as well as home and cellular phone numbers. Photos posted on teen sites were usually photos of themselves that could assist in locating them. Some of the photos are highly inappropriate if not provocative. It was not uncommon to see photos of teens involved in underage drinking, drug use, and risky behavior.

As Matt became friends with teens online, he had access to messages known as bulletins. These bulletins can only be viewed if you have friend status. Through these bulletins, I was able to gain much personal information about my online friends. Teenagers readily discuss their social activities and provide phone numbers to contact them. One time I saw a real-time message from a teen telling the exact location that she and her friends were about to walk to. If I had devious intent, I could easily stalk or intercept her and her friends. Many of the teens use bulletins to post surveys that reveal very personal information about them. Surveys that can be viewed by the general public are also a common sight on a teen's web page. In one case I found a 377-question survey on the site of one of my online friends, who was a 15-year-old female. This survey included the teen's personal information as well as her likes and her dislikes. These surveys assist predators in establishing a dialog with the teen as they attempt to infiltrate that teen's online world.

One of the most concerning incidents of the Matt online experiment occurred when one of my online friends suggested that we meet in

person. The in-person meet is the most dangerous scenario online. Teenagers meeting an online stranger sometimes become the victim of sexual assault or worse. The 16-year-old female that made the suggestion to meet in person communicated with Matt on a daily basis. This teen later said she allowed Matt to become one of her online friends because she saw that other teens she knew were also friends of Matt. I found that teens are very trusting of people they meet online and very willing to share their personal thoughts and information with virtual strangers.

As the Matt experiment was drawing to a close, three mothers of Matt's online friends agreed to share their child's online interactions with Matt with the Dateline NBC viewing audience. The three teen females, who were 15 and 16 years old, were unaware that they were part of the online experiment when they were interviewed by Dateline correspondent Rob Stafford. Stafford asked the girls if they provided personal information on their MySpace site and they told him that they did not post personal information. He also asked them if they would talk to a stranger online. The girls said that they would not. At one point in the interview I was brought into the room and introduced to the girls as Matt, their online friend. The surprised girls were then told about all the personal information that Matt was able to find out about them. The three girls could have easily been Middletown, Connecticut's victims eight, nine, and ten. They later acknowledged that they were relieved to know that I was a police detective rather than an adult looking to harm them. In this case, the girls were lucky.

In a 2-month period in the spring of 2006, some 17 Connecticut teen females were victims of sexual assault by people they met online. Some of these girls were young middle school students. Other locations throughout the country have had similar cases.

Another result of the Matt experiment was the way in which the teens' parents were totally unaware of what their teens were doing online. As I travel around doing parent programs on Internet safety, I see that many parents are not as technologically savvy as their children. Because of this, teens are often allowed to police themselves online. The Matt experiment as reported by Dateline NBC clearly shows that teens are very vulnerable online. It also demonstrated that parents are often blindsided by their teens when it comes to knowing exactly what they are doing online.

As technology changes, we will be faced with further challenges when it comes to teens' online safety. I see the next challenge being a web-enabled cellular phone. While parents struggle to monitor their child's Internet use at home, the cellular phone will provide Web access where monitoring will be difficult. The cellular phone now has

capabilities such as text messaging, instant messaging, email, and Web page access. Teens will now be able to leave their home and bring an extension of the home PC with them through their cell phone. Web cams will also become more common, leading to potential abuse as people will now be able to see each other while they are online. The ability of teens to have international friends online will pose an additional challenge to both parents and law enforcement.

There is no quick fix to the problem of online safety as it impacts our children. It will take vigilance by government officials, schools, law enforcement, Internet service providers, including social networking sites, as well as parents and teens themselves. I believe that industry standards as well as educational programs and public service announcements will go a long way as a first step.

Thank you.

[The prepared statement of Frank Dannahey follows:]

PREPARED STATEMENT OF FRANK DANNAHEY, DETECTIVE, ROCKY HILL, CONNECTICUT  
POLICE DEPARTMENT

Law Enforcement Experience:

- 25 years law enforcement experience
- 15 years serving as a Detective in the Youth Division
- Served in an undercover capacity to detect online child predators
- Seven years experience in Child Computer Crimes in both investigations and education

Dateline NBC Online "Matt" Experiment:

- Participated in an experiment which tested Middletown, Connecticut teens for vulnerability with a 19 year old online stranger
- Seven Middletown, Connecticut teens from the ages of 12 to 16 were victims of sexual assaults by older males met on MySpace.com
- "Matt," the role I played online, was easily able to make over 100 online "friends" in two week period
- Majority of 14 and 15 year olds with "private" pages allowed "Matt" on their page as a "friend"
- Personal information such as real names, where they live, home phone numbers, and actual dates of birth are readily given by teens online
- Use of "surveys" online reveal much personal information about a teen
- 19 year old "Matt" received a message suggesting an in-person meet
- Many parents not aware of what their child is doing online
- Many parents not technologically savvy about computers or the Internet

Future Challenges:

- Web enabled cellular phones will present new challenges in monitoring by parents
- Web cams will become more popular and lead to potential abuse by teens
- As social networking sites go international the potential to meet out of country friends will present new challenges

## Solutions:

- There is no quick fix for teen online safety
- Cooperation from multiple entities as well as parents and teens is necessary
- Industry-wide safety standards are necessary
- Educational programs are critical

Good afternoon Mr. Chairman Whitfield, Ranking Member Stupak, and members of the Committee, I am Detective Frank Dannahey of the Rocky Hill, Connecticut Police Department. I have been a member of law enforcement for the past 25 years; for the last 15 years, I have been assigned to the Youth Division of the Rocky Hill Connecticut Police Department. Over the last seven years, I have been involved in investigations and education concerning Internet Crimes Against Children. I have served in an online undercover capacity to detect Internet predators. My current efforts involve Internet safety programs directed toward parents, students, school officials, and law enforcement. In the past seven years, I have seen technology change in a direction that both benefits and assists online predators in carrying out their criminal activity. With the majority of America's teens online, the pool of potential online victims is vast.

In February 2006, an incident occurred in Middletown, Connecticut that attracted national attention. Seven teen females from the ages of twelve to 16 years were victims of sexual assault by older males they met on MySpace.com. All of these crimes occurred within a very short period of time. I was asked by the Middletown Police Department to assist them with parent education programs on Internet safety. As these programs for Middletown were being developed, we were contacted by Dateline NBC. Dateline was interested in profiling these crimes as well as reporting on the educational programs for parents. While preparing for the educational programs, I became involved in an online test of teen vulnerability. In a departure from the normal type of online undercover scenario, I took on the role of a teen male named "Matt." "Matt" was a 19 year old "new kid in town" who was looking for online friends from Middletown, Connecticut. In just two weeks, "Matt" had over 100 online "friends" on MySpace.com. I was particularly surprised and shocked to see that a majority of young teens, who were 14 and 15 years old, allowed "Matt" on to their "private page." The information on a "private page" is not viewable by anyone unless that person allows someone on as a "friend." Some teens questioned "Matt" about who he was before allowing him on their MySpace page as a "friend." Many teens allowed him on as a "friend" with no questions asked.

Once "Matt" was allowed on the teenagers' MySpace pages, it became immediately obvious that personal information was readily available and easily volunteered. I was able to find out information such as where a teen lived, worked, their full name and date of birth, where they went to school, as well as home and cellular phone numbers. Photos posted on teens' sites were usually photos of themselves that could assist in locating them. Some of the photos posted are highly inappropriate if not provocative. It was not uncommon to see photos of teens involved in underage drinking, drug use, and risky behavior. As "Matt" became friends with teens online, he had access to messages known as "bulletins." These "bulletins" can only be viewed if you have "friend" status. Through these "bulletins," I was able to gain much personal information about my online friends. Teenagers readily discuss their social activities and provide phone numbers to contact them.

In one case, I saw a real time message from a teen telling the exact location that she and her friends were about to walk to. If I had a devious intent, I could easily stalk or intercept her and her friends. Many of the teens use the "bulletins" to post surveys that reveal very personal information about them. Surveys that can be viewed by the general public are also a common sight on a teen's web page. In one case, I found a 377 question survey on the site of one of my online "friends," who was a 15 year old female.



This survey included the teen's personal information as well as her likes and dislikes. These surveys assist predators in establishing a dialogue with a teen as they attempt to infiltrate that teen's online world.

One of the most concerning incidents of the "Matt" online experiment occurred when one of my online "friends" suggested that we meet in person. The in-person meet is the most dangerous scenario online. Teenagers meeting an online stranger sometimes become the victim of a sexual assault, or worse. The 16 year old female that made the suggestion to meet in person communicated with "Matt" on a daily basis. This teen later said that she allowed "Matt" to be one of her online "friends" because she saw that other teens she knew were also "friends" of "Matt." I found that teens are very trusting of people they meet online and are very willing to share their personal thoughts and information with virtual strangers.

As the "Matt" experiment was drawing to a close, three mothers of "Matt's" online "friends" agreed to share their child's online interactions with "Matt" with the Dateline NBC viewing audience. The three teen females, who were 15 and 16 years old, were unaware that they were part of the online experiment when they were interviewed by Dateline correspondent Rob Stafford. Stafford asked the girls if they provided personal information on their MySpace site and they told him that they did not post personal information. He also asked them if they would talk to a stranger online. The girls said that they would not. At one point in the interview, I was brought into the room and introduced to the girls as "Matt," their online "friend." The surprised girls were then told about all the personal information that "Matt" was able to find out about them. The three girls could have easily been Middletown, Connecticut's victims 8,9, and 10. They later acknowledged that they were relieved to know that I was a police detective rather than an adult looking to harm them. In this case the girls were lucky. In a two month period in the Spring of 2006, some 17 Connecticut teen females were victims of sexual assaults by people they met online. Some of these girls were young middle school students. Other locations throughout the country have had similar cases.

Another result of the "Matt" experiment was the way in which the teen's parents were totally unaware of what their teens were doing online. As I travel around doing parent programs on Internet safety, I see that many parents are not as technologically savvy as their children. Because of this, teens are often allowed to police themselves online.

The "Matt" experiment, as reported by Dateline NBC, clearly showed that teens are very vulnerable online. It also demonstrated that parents are often blindsided by their teens when it comes to knowing exactly what they are doing online.

As technology changes, we will be faced with further challenges when it comes to teens' safety online. I see the next challenge being the web-enabled cellular phone. While parents struggle to monitor their child's Internet use in the home, the cellular phone will provide web access where monitoring will be difficult. The cellular phone now has capabilities such as text messaging, instant messaging, e-mail, and web page access. Teens will now be able to leave their home and bring an extension of the home PC with them through their cell phone. Web cams will also become more common, leading to potential abuse as people will now be able to see each other while online. The ability of teens to have international "friends" online will pose an additional challenge to both parents and law enforcement.

There is no quick fix to the problem of online safety as it impacts our children. It will take vigilance by Government Officials, Schools, Law Enforcement, Internet service providers including social networking sites, as well as parents and teens themselves. I believe that industry safety standards as well as educational programs and public service announcements will go a long way as a first step. Thank you.

MR. WHITFIELD. Detective Dannahey, thank you for your testimony.

From your personal experience as a detective in working on this issue of child molestation and child pornography, you have been giving these classes now for some time teaching Internet safety to parents and children or just parents?

MR. DANNAHEY. No, both parents, students, school staff, law enforcement.

MR. WHITFIELD. And how many classes have you taught would you say, first of all?

MR. DANNAHEY. I think over the 7 years, probably hundreds.

MR. WHITFIELD. And did you say that most young people today that are using the Internet really have an understanding of the dangers that they may face?

MR. DANNAHEY. No, they don't. I think it is very obvious that when you talk to teens, they will certainly acknowledge they have seen on the news some of these high-profile incidents. They will acknowledge that there are people out there that will harm teens online, but when you start getting personal with them and talking about their own personal Internet use, I think very often they have that "it is not going to happen to me" attitude and I think that part of the problem here is the not realizing that just what you have spoken about today can actually happen to them. It is something that always happens to somebody else.

MR. WHITFIELD. And have you found that most parents are not particularly technologically advanced as relates to the Internet?

MR. DANNAHEY. No, and I think that really contributes to the problem. I mean, when you look at all these different items of technology out there, look at a cell phone. I mean, most adults are lucky they know how to answer the cell phone, maybe make a phone call. A teen probably within 24 hours is going to know everything about that cell phone. They are going to read manuals, they are going to ask their friends whereas adults clearly may never know the capabilities of technology they have.

MR. WHITFIELD. So we generally have a situation where the young people are so much more advanced than the parents and so it is very difficult for the parents to even understand or comprehend what is going on.

MR. DANNAHEY. Exactly, and I think, when I speak to parents in these seminars I do, I often tell them, you don't have to be a networking person to have enough knowledge to monitor your own PC at home to see if your children are doing things that are dangerous. It is just a matter of maybe doing a little research, going to presentations such as the ones that I give and other law enforcement agencies give and just having some basics, and really, I often tell them that the best way to understand

the computer system is to ask the teens to give you a tour of what they do online.

MR. WHITFIELD. And the young people that I have talked to are all very excited about MySpace and they are excited about Facebook and they are excited about this social networking, but it is kind of perplexing as Matt, your fictitious character, you were able easily to enter into a dialogue with a lot of young people, correct?

MR. DANNAHEY. Yes, very easily.

MR. WHITFIELD. And I was a little bit puzzled by how these young ladies, for example, gave you a lot of personal information, but from their perspective, they did not view it as personal?

MR. DANNAHEY. Exactly. I think that the word that you use is very apropos. They don't necessarily perceive certain information as personal information. I often tell them, when you look at a particular web page, it is like pieces of a puzzle. When you go from different areas of the page, you extract information and somebody, again an online predator, certainly is very good at that and they will take little pieces of information, put them together and actually have a lot of information about the teen. But, when you talk about personal information, they don't see personal information in the same context as we see personal information. I think to them a personal information would be if you gave your street address and sent them a map to get to your house.

MR. WHITFIELD. And that is what they gave you. They gave you cell numbers, home numbers, where they worked, their address.

MR. DANNAHEY. Right. Everything they gave me without a lot of skills or knowledge would enable me to basically, as I said to them, go up and ring their doorbell.

MR. WHITFIELD. And many of these young ladies would have their picture on MySpace, and a lot of information about them. I had not heard of MySpace until about 3 months ago, to show you how backward I am, but I do know now a lot about it and I have been on the site, and I agree with you that a lot of the pictures are pretty provocative, so if you had a predator out there obtaining that kind of information, it would be relatively easy for them to meet some person.

MR. DANNAHEY. Absolutely. I think those teens, not to discredit all teens, there are some that don't give a lot of personal information out, but I think when you look at most teens' pages, the kind of information that you can extract off the page would give you a very good idea, exactly geographically where they live, and it wouldn't take very much research to find out where most kids live and go to the community. You have a photo there, show the photo to another teen or whatever. I am sure they would readily tell you the name of the person and where you could find them if you had the right story.

MR. WHITFIELD. Now, you mentioned something about real time. Explain that a little bit what you are talking about.

MR. DANNAHEY. With the bulletins, if you are at home and you are receiving one of these bulletins, these bulletins are sent in real time so if for example, the girls saying that they are going to walk to a very distinct restaurant in their community which would easily be located, it is in real time. So if I saw they were walking there and again from their information knew geographically where they were from, it would be nothing to get into a car and actually intercept them to where they are going.

MR. WHITFIELD. Absolutely. Now, have you contacted different social networking sites on their law enforcement links?

MR. DANNAHEY. Yes. In a couple weeks I am going out to speak at a national school resource officers' conference, and I wanted to have a basis to give my colleagues some information as to who they can contact for law enforcement assistance. I emailed three of them. I have not heard back from them. The fourth, MySpace.com, has actually published a law enforcement guide which I do have a copy of that I am going to share with the folks from the National School Resource Officers Association.

MR. WHITFIELD. But did these links respond?

MR. DANNAHEY. Not as of yet.

MR. WHITFIELD. Not as of yet?

MR. DANNAHEY. No.

MR. WHITFIELD. Now, when you talk to children--and when I have talked to children, they generally tell you--in fact, I had a group of 4H students in my office today and we were talking about the Internet and MySpace and Facebook, and they said well, we don't talk to strangers. I would ask you, what is a stranger to children online?

MR. DANNAHEY. Well, again, I think to us and them, it is two different definitions. I think when--for example, at the time we picked these three particular girls and, the Dateline correspondent, Rob Stafford, said, "Did you talk to strangers online?" Across the board they said no, and I think in their own mind they believe that. I mean, to them this was a guy that they met online. This is a guy--in one girl's case, I talked to her every day, so to her that wasn't a stranger. So I think that is what we have to get across to them actually--what is the definition of a stranger. All these people they have on their friends' pages when you start pointing particular people out, some they know from school and from their communities, others they will say, well, this is my friend from California or this is my friend from Pennsylvania; how do you know that; they told me that.

MR. WHITFIELD. The only thing they know is what you tell them and they never know nothing about you.

MR. DANNAHEY. Absolutely, but it is very true that an adult and a teen have much different definitions of what a stranger is.

MR. WHITFIELD. At this time my time is about expired here. I will recognize Mr. Stupak from Michigan.

MR. STUPAK. Thank you, Mr. Chairman.

The last part the friend where a friend from California or whatever, they may know nothing about them, has law enforcement tried to develop any kind of a checklist that young people should look at before they would do the friend status?

MR. DANNAHEY. Well, I think in my educational programs, I mean, we go over all these aspects of the Internet and that is exactly one thing that, myself and others who do what I do try to hammer home to them is exactly what the definition of a friend is. My view is that I feel that a parent or the teen themselves should be able to pinpoint each one of those friends and personally know who they are. I always tell the teens that if you just have one person on that page where you can't say you personally know them, then your safety has been compromised.

MR. STUPAK. But at the same time, you say you don't personally know them. Would that not encourage personal encounters?

MR. DANNAHEY. Well, I am talking about the people they know from school. I mean, my view of being safe online for teens is for them to speak to other teens from their school, from their community. When you start going outside of that, obviously now you are getting into these relationships where these friends are just online friends and not someone who you know anything about.

MR. STUPAK. And I have had this discussion with young people and they say well, then you defeat the whole purpose of the Internet because the Internet is supposed to allow you to go anywhere, so I can't have my friend in California if I live in Connecticut, then what good is it, and so it is sort of a tough one to deal with. In Connecticut in your area, does Connecticut require any cyber security classes being taught in school?

MR. DANNAHEY. No, I don't think there is any requirement for it. I think with all these high-profile incidents that have been in the news, I mean, they are certainly scurrying to do that right now. I know that in Connecticut I had far more requests to do programs than I could physically do.

MR. STUPAK. And that was a suggestion that came up yesterday. Would you endorse that kind of a--

MR. DANNAHEY. Absolutely. I mean, again, you know, organizations already in the school system like, for example, the DARE program which I am involved in, the school resource officers who are in

many of our schools around the country, it would just be a natural thing for them to add a curriculum, to those already intact programs. In my DARE programs, we several years ago decided to put an Internet component in and they certainly encourage you to do that. Same with the School Resource Officers' Association.

MR. STUPAK. As a school resource officer then, were you given training in this field?

MR. DANNAHEY. The school resource officers are the in-school police officers, and as part of their duties other than security, they are also required to teach a curriculum to the students whether they--

MR. STUPAK. In cyber security?

MR. DANNAHEY. There is no requirement right now, but it is certainly a suggestion, and from all the talk groups I am in, I see that a lot of them are doing that right now. There are curriculums that they have on their website for Internet safety and I think that is a big concern of that organization is to get that topic into the school system.

MR. STUPAK. One other thing. I am a little bit off subject here but last night on the floor we were trying to just maintain funding for law enforcement. We had a \$900 million cut in this budget. The Clinton COPS program was one that really developed the school resource--

MR. DANNAHEY. Yes.

MR. STUPAK. And after the Columbine incident, we had a lot of them but now we see funding has fallen off, and these hearings highlight the needs for things like school resource officers. Are you familiar at all with MySpace and the safety features they put out on or about June 21?

MR. DANNAHEY. Yes, I am familiar with some of the new changes.

MR. STUPAK. Like heightened security for settings for 14-, 15-year-olds, full privacy settings for all members and age-appropriate ad placements.

MR. DANNAHEY. Yes.

MR. STUPAK. Good first step. Do you believe they will make it any more difficult for you to repeat your exercise of Matt there, your 19-year-old?

MR. DANNAHEY. Well, I think that will certainly discourage, especially with these younger teens. I mean, I was very concerned about the fact of how many of the youngest of teens online of 14- and 15-year-olds, which actually a two-third percentage allowed this Matt stranger onto their private page. I think the steps they put in place would certainly discourage the ease of doing that. I am not saying it would be impossible for me to get onto a private page of a teen but it would certainly discourage that.

MR. STUPAK. In your estimation, what invites a teen to be Matt's friend? Your sympathetic story about being a young person and not knowing anybody or--

MR. DANNAHEY. Basically the story was that he was an older teen, a little bit of a troubled kid coming from another State and coming into a community where he knew no one and was looking for some friends and thought that the online way to go would be a great way to meet friends in that new community.

MR. STUPAK. Well, MySpace was maybe a good first step on some ideas they have to enhance safety. In your opinion, what other things would you like to see industry do to enhance safety on these social Internet places?

MR. DANNAHEY. I think what would really help if the social networking sites themselves had some industry-wide standard. The problem always is, especially when you are dealing with teens, if one of the sites is doing a great job of enhancing their security, I think oftentimes that might discourage their teens who are their customers from being on that site so they may gravitate to a site who has very lax standards. So being that they are all for-profit companies and need members to exist or whatever, I think if all sites had some very similar safety standards, that it would kind of be an even playing field. I would like to also see some of these third-party sites where they are allowed especially with these, like I told you this outrageous 377-question survey, they are bringing these types of things in from other sites other than MySpace and planting those on the page. I think the surveys just reveal far too much personal information that should not be given out by anybody.

MR. STUPAK. So that survey, I take it you took it as being a--to determine whether or not you would be a friend where you would elicit information from the person?

MR. DANNAHEY. Yes. In fact, that 377-question survey which is not based from MySpace but can be imported to their page, the second question is, what is your full name, and then the third question is, what is your date of birth, and in checking out all these teens for prospective candidates that might be willing to be televised, I picked a dozen of my 120 friends and when I went to their high school, I found out that all the information was true. If they said their name was such-and-such, it was that. If they said their date of birth was this month, day, and year that was true. Everything about their information actually checked out.

MR. STUPAK. It seems like that--you said two-thirds of them that let us be friends were 14- to 15-year-olds.

MR. DANNAHEY. Yes.

MR. STUPAK. It almost seems like sort of a gullibility or else maybe haven't been around long enough or life experience to put up red flags. It has been suggested that maybe 14- to 15-year-olds have a separate site like MySpace but only for 14- and 15-year-olds and have that protected. Would that serve better than just heightened security?

MR. DANNAHEY. I think if they are willing to accept that. As you said or somebody stated you get in this situation where they are altering dates of birth. Just on Monday I had a parent call me, not too Internet savvy. She had an indication that her daughter might have a Web page, and when I brought the page up and spoke to her over the phone, the daughter had a photo that was not hers. The daughter stated a date of birth that was not hers. When I looked at the friends, I clearly recognized them as middle school students. All the students on her page happened to be 13 years old, so of course, the mom was immediately going to have the girl take the page down but, that is part of the problem, them misstating their date of birth. Would they go to the 14- and 15-year-old-only site? I am not sure that they might do that.

MR. STUPAK. There has got to be a way that you can enforce this somehow. I mean, with all the technology we have now, there has got to be some way to verify it, I would think.

MR. DANNAHEY. Well, I know that there is software out there that looks for key indicators when you misstate your age but somewhere else on the page you actually state your real age and they are detecting that, so I know I have read that. You know, MySpace has taken down pages when they do find that scenario.

MR. STUPAK. In your testimony, you mentioned some of the challenges we'll have in the future, and one of them was the cellular phones. Do you want to explain that a little bit more?

MR. DANNAHEY. Well, the problem with the cellular phones is, there is not--I mean, especially with the high-end sophisticated ones, which the teens tend to have, there is not a lot of things that you can't do with that Web line that, it kind of mimics the home computer. Now, of course, you have often heard that probably one piece of information you are going to give to a parent doing an educational program or a public service announcement would be, keep that computer in a public place. Well, now, having a cell phone that can very much duplicate what a PC does, how do you instill it upon the teens to do all those safety rules that they would normally do at home when they are going out the door clipping the cell phone on their belt and saying see you later, Mom, and now have unrestricted use of this without being monitored. I think that is going to be a real challenge.



MR. STUPAK. My last question. What advice did you give to teens regarding these social networking sites? If you are teaching a class, what is your best nugget as to what you tell teens on this whole thing?

MR. DANNAHEY. The first thing I tell them is, I am not opposed to these sites. I think teens are going to use the Internet. It is just that you have to maintain your personal safety. No one is going to do that for you. Your friends need to actually be your friends. The moment you have somebody on your page, a buddy list, a friend list, that you can tell me you don't know personally who they are, you have immediately compromised your safety. So I think it can be done. I know a lot of parents work in cooperation with their teens, a little bit of a checkup without being overly nosy to make sure they are safe. I really think it can be done but, just as the industry has to take steps, I think the teens and the parents also have to be part of this or it is not going to work.

MR. STUPAK. Thank you.

MR. DANNAHEY. You are welcome.

MR. WHITFIELD. Mr. Walden. Oh, Mrs. Blackburn. Okay.

MRS. BLACKBURN. Mr. Chairman, thank you.

Detective Dannahey, you know, this is such a complicated issue and I really do appreciate your taking the time to be here with us and talk with us about it. Being a parent and having been a room mother and Sunday school teacher and those things, you look for ways to be certain that you help children learn to socialize, and you try to communicate the message that home is a safe place and items contained in the home are a safe place, and then in the classroom with the advent of computers coming into the classroom, we tried to teach our children that this was a great way to explore and a great way to experience the world at your fingertips, and it is so interesting to see the evolution of the social networking sites. I remember a couple of years back when I was asking about someone, and my son, who is now 25, said well, just go look them up on Facebook. I had never heard of such. And I was absolutely appalled that that much information could be available to the world about young people.

And I have got a question for you, but what you just said is so very true. It is teaching children how to maintain their personal safety but at the same time having them realize what the dangers are, what the vulnerabilities are. And why do you think that teens today, especially these younger teens, have absolutely no fear or recognition of the danger that is there when they place things on the Internet? Why is there just no awareness of the danger?

MR. DANNAHEY. I think that goes back to my comment on having worked with teens for 15 years, they definitely have that "not me" feeling. The best example I can give is if you think about a community

having a tragic drinking-and-driving accident where a student is killed because of alcohol. You will clearly see that for a short time the underage drinking parties will stop, teens' awareness of drinking and driving will be heightened, but I have to say that probably after a couple months, after a few months that all goes away and, the parties continue, the drinking and driving continues. So I think it is very difficult, especially among that age group, to relate things to them personally. I think they will acknowledge bad things happen but they will often say bad things don't happen to me, bad things can't happen to me.

MRS. BLACKBURN. Do you receive a similar type of response from the parents when you are holding the sessions with them?

MR. DANNAHEY. As far as their own teens' vulnerability?

MRS. BLACKBURN. Yes.

MR. DANNAHEY. I think it is a much different picture. I think parents are scared to death out there, especially the ones that aren't that Internet savvy, don't understand anything about being online, or don't understand anything about the computer. They are just sponges for knowledge. You know, it is unfortunate that when you do these programs that very often the kind of parent that is going to show up for an Internet safety program is the parent that doesn't need to be there. Those kids whose parents should be there aren't there. I mean, I often say that even though you might have 25, 30 people in the room, sometimes the domino effect will pass that information onto somebody else but, even with those high-profile incidents I went out to different locations that had the problem, had the big news headlines, and you would think the auditoriums would be full and they weren't.

MRS. BLACKBURN. I have talked to so many parents in my community who have just been captured with the sense of disbelief when they realize what is available or what their children are putting on the Internet and are really quite concerned about, and we have had some great discussions, and I hope that does lead to some awareness.

I wanted to go back. You mentioned the DARE program. I am a big fan of DARE programs. I think they work. They yield results and they are time well spent. And you mentioned that you had inserted an Internet component and that you had a checklist. Can you kind of click through that checklist or could you submit that to us just for the record?

MR. DANNAHEY. Yes, I could certainly submit my curriculum. I think when you start at an early age, you might have some results. Obviously, when I go out, especially right now, you are talking to juniors and seniors in high school about Internet safety. You have to have a different slant because, again, they, at that age feel that they are invulnerable, that nothing is going to happen to them. I think once you start especially in the 5<sup>th</sup> and 6<sup>th</sup> grade, at least we have a chance to instill

that. I mean, you see the tobacco use by children, you see those statistics going down. I would like to say that maybe programs like the DARE program should take credit for that and I think we can do the same thing with Internet safety that we have done with tobacco education and start in the early grades, like in 5<sup>th</sup> grade, 6<sup>th</sup> grade, or maybe even 4<sup>th</sup> grade talking about the computer. The fact that it is that great tool but it also comes with some dangers assigned to it also.

MRS. BLACKBURN. Thank you so much. I will look forward to that list, and thank you for your work and your dedication.

MR. DANNAHEY. You are welcome.

MR. WHITFIELD. Thank you, Mrs. Blackburn. I recognize Ms. DeGette.

MS. DEGETTE. Thank you, Mr. Chairman.

Detective, I am wondering, you talked in your opening statement about having parents have their children show them what they do on the computer but I am wondering if you can say more specifically what exactly you tell parents that they can do to protect their children from these predators on these chat rooms and other sites?

MR. DANNAHEY. One of the first things I tell them is, you have to get some kind of education. There are several safety sites out there. I give them a list of maybe half a dozen of the best of the best to go to, to kind of get an education of, in simple terms, what does this term mean, how do you do this, how do you do that. I wrote up a very basic, as I call it, parent computer forensics 101, showing them step by step how they can monitor their hard drive, and a big portion of that is, I tell them that they have to communicate with their kids. It is kind of a sneaky way but, if you do sit down and say to your teen, hey, show me what you do online, show me a little bit about the computer, you get a great indication of how computer savvy they are. Some kids aren't that computer savvy and maybe have a little bit of a comfort zone. Other kids will zoom around there with that mouse and keyboard and you know you might have to do a little bit more monitoring. But I think the communication part is huge.

MS. DEGETTE. One thing I was just sitting here thinking, you could--if your kid is in these chat rooms, you could ask him to show you their buddy list and you could say who are these people. Would that be effective?

MR. DANNAHEY. Absolutely. The three girls that we picked to appear on that Dateline show, all of them have MySpace pages today, all of them are on private, all of them have their moms as their friends. Now, the moms--obviously there was a lot of work to do after that show aired to get their sites safe again--but every single one of those friends, the moms went, person by person, who is this, how do you know them.

The moms periodically will go in and check, not to the point again of being overly nosy, reading every little message, every little thing, but I think a setup like that can work if a parent and teen does it in the right way and I think that is the only solution is to have this collaborative agreement between both parents and teens to yes, you can have a social networking site, I have to have some partnership with you. Again, not overly looking at everything they do but just enough to see those in-your-face-type violations which they might have to--

MS. DEGETTE. Parents just need to realize that the same precautions they tell their children in every aspect of life, and you are right, you have to talk to them about drinking and driving and smoking every few months. You have to do it with computer safety as well.

MR. DANNAHEY. Exactly, and a lot of times I relate that to them as the 16-year-old approaching driving a car. I can't imagine any parent out in the audience would just give your 16-year-old a set of car keys and say go for it. There is a lot of preparation for that, and this has to be under the same terms.

MS. DEGETTE. One thing that we saw yesterday and maybe some people in the audience were here yesterday, a public service announcement. Mr. Chairman, I don't know if you are planning to play that again today.

MR. WHITFIELD. Well, after the second panel, we are going to do that.

MS. DEGETTE. Well, there was a public service announcement that was developed by the England--it was in the U.K. to warn young teens about what could happen if they are being preyed on and what to do. Have you seen that? Do you know what I am talking about?

MR. DANNAHEY. I believe if it is the same one that ran just a short time ago before this hearing. I did see that.

MS. DEGETTE. It is the young girl and it goes backwards.

MR. DANNAHEY. Yes.

MS. DEGETTE. Yes, it is a very, very powerful and effective commercial but I bring that up because, number one, I think that we need to have sort of not just parents talking to teens and people going in the schools but I think that we need to have a national public service program that the media outlets and if Congress can help in some way and ISPs and the other computer providers should do. Would that make sense to you?

MR. DANNAHEY. It would make a lot of sense. I think that is a great first step. I think that teens are very willing to make some changes once they see what you are talking about. I mean, after doing a student program, I mean, I get feedback from teachers saying wow, there was a

lot of buzz in our classroom after that. Teens are going to go home and change their page.

MS. DEGETTE. But, you know, teens don't want to--I mean, Mr. Inslee and I were just taking. Teens don't have the life experience that we have, and that is true in every way, but they don't want to put themselves at risk and so they are going to try and do--

MR. DANNAHEY. Exactly.

MS. DEGETTE. But the reason I bring up that particular PR campaign in Great Britain is because what they do is, they have systems which are used by all of the ISPs and it is in Great Britain and in Australia where they have a little logo, like when you are in a chat room, you have the--it is called the VGT, the Virtual Global Taskforce logo, which here you could do with--and it is a link to this global taskforce, so if you are in a chat room and you are having a chat and you are a 13- or 14-year-old girl or boy and you are starting to feel uncomfortable like maybe somebody is making some advances that are inappropriate, you can click right on that icon. You can go right into that law enforcement website. They capture the page and then they can go and investigate it. Are you aware of that kind of enforcement technique?

MR. DANNAHEY. No, actually I just heard about that today. That was the first time that I heard that. Other than the National Center's tip line, I am not aware of any other similar thing going on.

MS. DEGETTE. I mean, National Center has a tip line too but in Australia and Great Britain, all of the Internet service providers do this on these chat rooms and it is a fairly--it is staffed 24 hours a day so if some teen is on the Internet at 3:00 in the morning in a chat room and she gets solicited or something and it makes it uncomfortable, all they have to do is hit that button and it goes straight--do you think that it would be helpful for the ISPs to develop some kind of a system like that in conjunction with the Center for Missing and Exploited Children here?

MR. DANNAHEY. I think so. My only question would be, would the ICAC taskforces and, you know, National Center be, staffed enough to handle--I mean, being the number of people we have in America, teens in American online, I don't know if they would be overwhelmed with complaints. I think given the proper staffing, I think that could be a very really valuable tool.

MS. DEGETTE. And that might be a place that Congress could help out. I mean, one thing we do in these hearings which is very effective is, we raise the level of public consciousness, but frankly, every single thing we have been talking about here today is not something that we are going to legislate, but one place Congress might be able to help is in conjunction with ICAC and these other agencies to develop a system that perhaps we could use some public funding to help.

MR. DANNAHEY. Right, and I think with those agencies in place those would be the two logical agencies where you would do that kind of thing.

MS. DEGETTE. Right. Just one last question. Mr. Stupak asked you if you could do a separate chat room that would be targeted at younger teens, 14- and 15-year-olds. Given the fact that people can fairly easily circumvent the age registration requirements, would you be worried if we went to that type of website that predators might just be able to focus even more laser-like on younger teens?

MR. DANNAHEY. That is also the danger. I am sure parents would welcome that but again, I think what we have to realize is that teens aren't necessarily going to put the proper information in. If this is not looked at as a cool site--I mean MySpace is looked at as a very cool site. It is a status symbol at school to have a MySpace site. So if you broke away and had this 14- and 15-year-old site and that was not a cool site to have at the time, you might run into--

MS. DEGETTE. Right. I was the one that said that and I actually saw my 12-year-old go in her older sister showed her how to put a birth date that made her seem older than she was so she could get into some website and now neither one of my girls has a MySpace site but--

MR. DANNAHEY. I think they can though--

MS. DEGETTE. Heaven knows, they might have something else.

MR. DANNAHEY. I will give you my cooperative agreement if you like.

MS. DEGETTE. Yeah, okay. Thanks. I yield back.

MR. WHITFIELD. Dr. Burgess.

MR. BURGESS. Thank you, Mr. Chairman. I just want to thank the witness for being here with us today.

MR. DANNAHEY. You are welcome.

MR. BURGESS. In so many ways, I am glad to see you because we have been through this problem at so many different levels from victims to Internet service providers, and even had the Department of Justice in the room at one point, but what has really been lacking in all this is, is anyone who is interested in enforcement. We have had plenty of people who wanted to come in and talk about the problem and how bad it is and we all recoil in horror at how bad it is but this was really, but you are really the first witness that I can recall having come in to offer us some concrete suggestions, so I appreciate what it is that you do.

MR. DANNAHEY. Thank you.

MR. BURGESS. I do feel compelled to ask a question. I didn't get a chance to ask questions of the individual from Dateline yesterday. They seem to be awfully successful in recruiting individuals to come and misbehave at their sites. Do you think that is because they have the

production staff and they know what they are doing from just putting on the production, if you will, and so they are very professional, very clever at that, or do you think just someone who wanted to do this and identify those individuals would be just as successful because the pressure from the predator community is so intense?

MR. DANNAHEY. I think that is exactly right. Back when I did this fairly actively several years ago, the number of people we were going to investigate was only limited by the hours of the day, and I think you catch these guys and you pose the question, didn't you think it might be a police sting, and very often they will say yes but I also thought it might be a teen.

MR. BURGESS. Again, that is just an incredible concept. I know we have one individual, not in my district but close by in Jacksborough, Texas, who is a county sheriff and that is all he does, and it seems like with that small of a department would have a limited budget and yet they are putting someone on this continuously. It clearly deserves more attention than it has been getting from the enforcement community and I am particularly talking about at the level of the Department of Justice. Do you think that self-labeling and self-policing, children rating and reporting their own and other kids' websites for inappropriate content, do you think that is an effective way to go about policing these sites?

MR. DANNAHEY. I think it would be a tool, but if that was the only tool, I would be nervous about that because that is not an age group that likes to tell on each other, and unless it was a real serious type of incident or something that really scared them, I don't think they would be so willing to be telling adults that somebody did something online.

MR. BURGESS. The concept that the gentlelady from Colorado was talking about with the child being able to go on and clicking on an icon after receiving what they perceive as pressure from someone, kind of analogous to a click it or ticket, I guess, is that--because of jurisdictional issues in this country, how effective in fact would that be, or would in fact you need the involvement of the Department of Justice to adequately prosecute that across State lines, across jurisdictional lines?

MR. DANNAHEY. Well, I think as far as our country goes with these Internet taskforces, they are in all 50 States or cover all 50 States, that wouldn't be a problem. The problem lies then when you get what is that person is from the international community. Who is going to cooperate with U.S. law enforcement in something like that? They may put that name in a database. Would they do anything? It depends on what country that that person was from.

MR. BURGESS. So the unintended consequence may be to drive a good deal of this activity offshore but still have it go on?

MR. DANNAHEY. Unfortunately, that is another aspect of the social networking sites. When you have people on in the international community, I think we are going to start seeing some more incidents that we saw maybe several weeks ago of the stellar student, 16-year-old, going to the Middle East to meet a 25-year-old man. I think we are going to see more of that.

MR. BURGESS. From just the perspective of a parent, what advice would you give from what you have seen and what you have worked with, what is the best way for a parent to circumvent this? Never buy the computer in the first place?

MR. DANNAHEY. Well, if you tell them they can't have a site or if you tell them they can't be on the Internet, my worry about that and in talking to teens telling me exactly that would be that they will go underground. I think you have to have this somewhat cooperative agreement with your teens where you might not be 100 percent happy that they have their sites, but if the teen would allow you to at least maybe help set the site up for them, make sure it is safe, occasionally monitor the site, again not being overly nosy, I think that could work. But I have seen far too often where a parent will just come home from a seminar given by one of my colleagues that says throw the computer out the window and they will have the teen right in front of them take down all their social networking sites or Internet in general and that the teen will reemerge with new sites, new email addresses that the parent doesn't know anything about. So I think that cooperative agreement has to be there. Plus the fact that parents really have to get on the ball and just understand this technology. As I mentioned about these cell phones, I think they are going to be a huge problem because they are going to have all these bells and whistles and capabilities. A parent is going to allow the teen to buy these and they are going to have absolutely no idea what the capabilities are.

MR. BURGESS. During some earlier testimony, the question came up to one of the young men who was actually a victim, and the question was posed, is there any reason for a 15-year-old to have computer hardware that allows a video camera. Do you have any feeling about any type of age-appropriateness or restriction that should be placed on any type of hardware or peripheral that is attached to the computer?

MR. DANNAHEY. I think you are probably talking about Justin Berry, whose case I am very familiar with, a tragic case. I think as of right now, I would caution parents to not allow those devices where you can actually see the other person on the other end unless you have a really good reason to. I know some of the teens told me they have families in international countries and things like that but really, from what I have seen of these webcam sites, it is just clearly an indication for



abuse. When you do a web search on teen webcam sites, you will be horrified by what is going on. Just like Justin Berry, there are probably hundreds if not thousands of other teens out there seeing how you can actually make money on these sites and doing unspeakable things with these webcams. So I don't really see the need for most teens to have that and I think they are a big potential for abuse.

MS. DEGETTE. Will the gentleman yield?

MR. BURGESS. I just want to follow through on one thing. We require a package of cigarettes to have labeling on it. Should we require similar labeling on video reproduction computer peripherals?

MR. DANNAHEY. I don't know if that would do any good because you have got parents who don't read the manuals to the computer and the cell phone so I don't know. I think really our best bet is these education programs, public service announcements to get the word out there to parents of really what is going on out there. I don't know if that would do any good. But I think like Justin Berry's story, parents in the seminars that I do were just appalled by that. I bring that case up as well as some similar ones, and they can't fathom the 13-year-old being able to do something like that.

MR. BURGESS. I wasn't aware myself what came with the manuals. I will be happy to yield.

MS. DEGETTE. I was just going to say that the increasing use of these cell phones is going to make it even worse because even if you take the web cam out of your house, when these teens have the cell phones that will make movies and transmit them simultaneously, then you are going to have that same problem.

MR. DANNAHEY. Absolutely, and there have been some horrific cases with those phone cams or whatever where the teens are generating their own pornography out there, emailing them to boyfriends, girlfriends, and then of course, those relationships don't last forever and you see plenty of sites out there, ex-girlfriend sites, ex-boyfriend sites, and they are putting these photos online and are forever going to victimize the teens.

MR. BURGESS. Reclaiming my time. I guess my understanding is, Apple Computer has a built-in imaging device now which I guess is a good idea. The gentelady from Colorado also brought up--and I apologize if I was out of the room when you answered. What about the ability to take down a site or a picture once it has been inappropriately placed on the Internet? Is there any way to erase those images?

MR. DANNAHEY. No, there is not. I mean, unfortunately, there is no magic way of reaching out to the Internet. Early in the school year last year I had a 13-year-old girl take some just horrendous photos of herself that would absolutely be classified as child porn, mails them to a

boyfriend, and the boyfriend unfortunately shared his password and somebody got in and stole the pictures and established a website with these photos on it. She was horrified when she actually received a link to her own pictures and her first question, how do I take these pictures down. Well, we got the pictures off the website but how many people downloaded those photos? I don't know. I mean, she could be 25 years old and someone might walk up to her with one of her images and say this looks a lot like you. So that is a danger for teens. You cannot recall a photo once it is out there, and the pedophiles trade that and if it is homegrown-type photos, I mean, that is treated like gold. Anybody who has her pictures could probably trade those for all kinds of photos because they are of an actual real live 13-year-old girl.

MR. BURGESS. Thank you, Mr. Chairman. I will yield back.

MR. WHITFIELD. Detective, as you conclude here, I would like you to just take a couple of minutes to relate to us the story about the young girl who actually went to the Middle East to meet someone. I don't remember those facts and I was wondering if you would convey them to us.

MR. DANNAHEY. I am not sure exactly what State she was from, maybe out the Chicago way. She was a 16-year-old girl, by all accounts a good student, somebody who her parents would trust. She did communicate online with a person. I believe he is from the West Bank, a 25-year-old male, and somehow, as teens often do, she was able to convince her parents that she needed a passport, concocting a story that she was going to Canada with friends, got herself a passport, somehow got airline tickets, was flying to meet this guy, and once law enforcement apparently got into the computer and found out what was going on here, they intercepted her in Jordan and fortunately talked her into going home. Because I don't know, at 16 in a foreign country like that, I don't know if you put it to her and she said no, I don't know if you could actually stop this girl. And the 25-year-old male was seen in the media saying that he intends on marrying this girl and he intends on keeping this relationship going. And obviously for law enforcement and parents, it is just a scary situation where you may have our teens go to a country who has no ability or necessity to follow U.S. laws and may not cooperate with us. So you may have a teen in another country and literally we can't get them back.

MR. WHITFIELD. Are there any other questions for Detective Dannahey?

MR. BURGESS. Mr. Chairman, if I could, I just wanted to point out down in Dallas near my district, the Dallas County Child Advocacy Center is putting on a program next month called A Walk in Their Shoes, talking about these sorts of issues, and one of the sponsors is the

MySpace folks. So there are some good things that are happening out there and I certainly don't want to leave the people watching this with the impression that nothing good is happening. It is going to take a lot of that kind of work, however, as you have so eloquently outlined, to get the information out there and get it into the hands of parents who need it.

MR. WHITFIELD. Thank you very much for taking time to be with us today. We appreciate your testimony and wish you the very best as you continue your great job in this regard.

MR. DANNAHEY. Thank you, Mr. Chairman. I appreciate the invitation today.

MR. WHITFIELD. At this time, I would like to call the second panel, and on the second panel, we have Mr. Chris Kelly, who is Vice President of Corporate Development and Chief Privacy Officer of Facebook.com, Palo Alto, California. We have Mr. Michael Angus, who is the Executive VP and General Counsel, Fox Interactive Media, MySpace.com, Beverly Hills, California, and we have Mr. John Hiler, who is Chief Executive Officer of Xanga.com, New York, New York.

I don't even have to go through my spiel anymore. Everybody always knows. So if you all would raise your right hand.

[Witnesses sworn.]

MR. WHITFIELD. Thank you very much. You are now under oath, and Mr. Kelly, we will recognize you first for your opening statement. Do any of you want to be represented by legal counsel in your testimony today? Okay. Mr. Kelly, you are recognized for 5 minutes for your opening statement.

**STATEMENTS OF CHRIS KELLY, VICE PRESIDENT, CORPORATE DEVELOPMENT AND CHIEF PRIVACY OFFICER, FACEBOOK.COM, INC.; MICHAEL ANGUS, EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, FOX INTERACTIVE MEDIA, MYSPACE.COM; AND JOHN HILER, CHIEF EXECUTIVE OFFICER, XANGA.COM, INC.**

MR. KELLY. Thank you very much, Mr. Chairman, and we appreciate the presence of Ranking Member Stupak and the rest of the committee for this very important hearing on how to more effectively protect kids online through social networking sites.

My name is Chris Kelly. I am the Chief Privacy Officer of Facebook, a social utility that allows people to share information easily within their real-world community, and that is a very important emphasis point that will run throughout my testimony here today.

I joined Facebook last September as the first chief privacy officer in the social networking industry to continue the work that our founder,

Mark Zuckerberg, had put together in segmenting networks and protecting different communities online. I am creating the role at an Internet for the fourth time. In my previous service as chief privacy officer and a technology attorney, I have represented many clients in the technology and media industries on privacy, security, safety, and intellectual property issues. I was also part of the founding team and served as a fellow at Harvard Law School's Berkman Center for Internet Society, a think tank focused on public policy issues of the digital age.

I am very happy to be here today to talk about social networking sites generally but particularly about Facebook. By now a lot of you have heard a lot of bad things about what goes on, so I want to talk first about what good is going on and why these sites are so attractive to teens and older teens, and we started as a college site and it has expanded into high school, and then what is special about Facebook and especially our approach to safety.

Facebook is about community. It is about providing an online way for people to communicate with their friends and to meet new ones who are part of their real-world community. It is about providing individuals with avenues for self-expression and creativity and it is about providing community members with easy ways to learn and share new ideas. This is why it is so fun and popular with teens and college students, and now also we validate based on work communities.

I will run through in great detail the four levels of protection that we use to validate members onto our network, validate them into particular communities, protect the viewing of profiles. You have heard a lot about information being available on the open Internet. Facebook doesn't work that way. Membership on Facebook and the information on Facebook is available to individuals in validated communities by default and then later on by confirmed friends. So although founded only about 27 months ago by Mark Zuckerberg, our CEO and founder, in his dorm room at Harvard, modeled after the paper Facebook that everybody gets when they started college and as many Members of Congress get when they start in Congress.

We now have 8 million registered users. We are the seventh-most used website in America, according to comScore Networks, and we are America's most used photo site. There has been some suggestion that one of the reasons that you haven't heard about a lot of safety issues around Facebook has been because it is not as popular, but the comScore numbers tell a different story and I think it is because of the work that we have done from the beginning to segment networks and to work very hard at providing technological protections for our users that we haven't seen the type of safety incidents on Facebook that we have seen on many other sites.

So Facebook at its inception understood that communities must feel safe in order to thrive. There is a radical difference between sites that allow information to be posted to the open Internet and those which segment it within different communities. So our founders placed user privacy, security, and safety at the center of our mission and our architecture. So let me tell you how we implement these safety principles.

We implement our safety principles with four levels of user protection. Initially when you try to get on a network, we require validation where we can for high schools as well as colleges. We require a dot.edu email address or a dot.org email address for a number of high schools. I personally was a little bit surprised at the number of high schools that actually issue email addresses to their students. Where that is the case, a high school student cannot get on the Facebook site unless they have an institution-issued email address from that high school.

Then there is a second level of protection. Once you get on the network, you are segmented into a particular community, so for instance, if you were to join a particular high school community, by default you only have access to profile information to individuals within that community. So if you are searching for friends, this has two effects. One is, it limits the amount of information that one can reach, and two, it means that there's a built-in neighborhood watch program. We have a report this user, report this link, report this photo on every page in Facebook and our 20-person customer service staff can easily process complaints about somebody who is not in the network. They can launch an investigation and they often remove members who improperly get into a service. So we also empower our members to make choices in what they display on their site and to whom they display it.

We have very detailed privacy settings and choices and we also use technological monitoring tools to look at possible indications of antisocial behavior on the site. If somebody were to circumvent the two levels of protection that we have already set up and get through to a third and start to try to befriend too many people, try to reach out and get rejected friend requests, that is one of the things that we measure. It highlights a user account and allows us to investigate that. If the user is improperly on the service, they are shut out completely, and this has a real sanction because of the validated address in most cases because you can't just go and create another site with another email address. It is very difficult to get in.

So finally, we have this safety net with the humans and with our 20-person customer service staff that responds to the complaints as they come through that addresses possible violations on the site and looks at that, and then ultimately myself, our general counsel and two other

attorneys we have on staff interact with law enforcement if it ever gets to that, which it rarely does.

So as a result of these very important privacy, security, and safety features, we have very rarely encountered the same unfortunate problems that you have seen from most other social networking sites. We recognize, which is why we built the system this way, that there are bad actors out there, that they want to get into sites that have kids on them. Just like in the real world, you have to protect your communities in an effective fashion. So we vigorously sought to build these safety features into our product. We have also engaged in support of the educational and law enforcement efforts of the Federal Trade Commission, the National Association of Attorneys General, local law enforcement, non-governmental agencies like the National Center for Missing and Exploited Children and WiredSafety.org, and parents everywhere. We think that there are multiple levels of defense that all need to be deployed to protect kids online. We support the efforts of everyone in the social networking industry to take safety seriously and to upgrade our practices to make the world safer and more secure for the members of all these sites. So we think that competition to provide safety on these sites is a good thing for the industry and for the kids of America.

So for these reasons, Facebook, we commend this committee for holding these hearings. We are very excited to engage with you in this practice. We welcome the opportunity to continue to serve as a resource for you and would like to leave myself open for questions.

[The prepared statement of Chris Kelly follows:]

PREPARED STATEMENT OF CHRIS KELLY, VICE PRESIDENT, CORPORATE DEVELOPMENT AND CHIEF PRIVACY OFFICER, FACEBOOK.COM, INC.

Thank you Chairman Whitfield and members of the Subcommittee for this opportunity to be with you and explain how Facebook uses technology and policy to protect people on our network.

My name is Chris Kelly, and I serve as Chief Privacy Officer of Facebook, a social utility that allows people to share information with their real world communities. I am very happy to be here today to explain how the two core ideas of social interaction and privacy guide everything that we do, and help protect people on our network. As we say in our basic statement of principles on the site, people want to share information with their friends and those around them, but they don't necessarily want to share personal information with the entire world.

I joined Facebook last September as the first Chief Privacy Officer in the social networking space, and am creating the role at an Internet company for the fourth time. In my previous service as a Chief Privacy Officer and technology attorney I have represented many clients in the technology and media industries on privacy, security, safety, and intellectual property issues. I was also part of the founding team and served as a Fellow at Harvard Law School's Berkman Center for Internet and Society, a leading think tank focused on public policy issues of the digital age.

In February of 2004, our CEO and Founder Mark Zuckerberg launched the first version of Facebook from his college dorm room. Now, Facebook is the seventh busiest site overall and runs the busiest photo site in the United States, according to independent service ComScore Networks. We have more than 8 million registered members for whom Facebook has become a core part of how they interact within their communities. Starting with our college communities, we have since expanded to offer school-focused interactions for high-school students, and more recently have followed our graduating students into the work world.

Privacy, security, and safety have been at the forefront of our concerns since the founding of the site. There is one overarching way that Facebook differs from nearly all other social networking sites – profile information is not generally available to the outside world. It is only available to Facebook members inside their individual, validated networks or through confirmed friends. We want to give people extensive power over their ability to share information, and the ability to limit who has access to it.

Of course, no protection mechanism is perfect. But the mere fact that Facebook does not make information available by default to anyone with access to the Internet, combined with the other prudent measures we have taken to focus information sharing on real-world communities, has made a radical difference in the privacy, security, and safety of the Facebook experience.

Following this major differentiator from most sites, we have set up four levels of protection for our members that I would like to outline for you today.

First, we require validation in order to get on the site in the first place. For college students, and those high schools where it is possible, membership in the school community is proven through a valid email associated with that college or school. Where high schools do not offer students email addresses, we have instituted an invitation-based system that is designed to limit even initial access to that school network.

Second, we segment information access within networks based on real-world communities. Being a member of Facebook does not give you access to the profiles of all people on Facebook. You are only allowed to access the profiles of other members at your college, high school, work, or (with explicit user choice) geographic network, and have power to add confirmed friends in other networks. This has two positive effects. First, users are gaining more information about those around them in the real world, which has pro-social effects on campuses around the country. Second, there is a built-in neighborhood watch program, especially with respect to high schools, where abuse of the system can be easily identified and addressed.

Third, we put power in our users' hands to make choices about how they reveal information. I have mentioned already the ability to confirm friends from other networks, and the "My Privacy" tab on every navigation bar throughout the site allows users to make detailed choices about who can see particular pieces of information about them, including their contact information and photos.

Finally, we have a safety net of protection through both technological tools we deploy to detect misuse of the site and human capital dedicated to potential problems -- our 20 person and growing customer service staff, headed by a seasoned veteran and backed up by myself and two other attorneys. Most of our customer service representatives are recent graduates of outstanding colleges, and dedicated Facebook users, so they know the system inside and out. On those rare occasions where someone has attempted to misuse our network, we engage rapidly with the relevant authorities. Because the system is built for accountability with its email validation requirement and segmentation of communities, misuse is both deterred and generally detected quickly. We quickly launch an internal investigation and step in where we receive reports of the misuse of Facebook in any way.

Overall, the fact that information posted on Facebook is not generally available has made Facebook a different experience for our users, and one they clearly enjoy as

reflected in their frequent visits. Our intuition about the importance of tying access to information based on the networks where people already exist in real life has been shown to have huge effect in both deterring and exposing misuse. By focusing on real-world networks as the touchstone for access, we provide both a built-in reflection of people's expectations about who will know information about them, and restrictions that make access difficult for those who might have harmful intentions.

Facebook is proud to have led the way in giving people control over sharing information online. Thank you again for the opportunity to comment before the committee, and I look forward to your questions.

MR. WHITFIELD. Thank you very much, and Mr. Angus, you are recognized for a 5-minute opening statement.

MR. ANGUS. Thank you, Mr. Chairman, Ranking Member Stupak, members of the subcommittee. My name is Michael Angus. I am the General Counsel of Fox Interactive Media, parent company of MySpace.

I want to thank you for inviting us today to address concerns about Internet safety and to discuss how we can collectively protect younger users on the Internet.

Safety and security have been a priority for MySpace prior to the acquisition by Fox and continue to remain a top priority at the highest levels of our company. We take seriously our responsibility to provide a safe and well-lit space for our community, not only because it is the right thing to do but because it also makes good business sense. It is what our community and our advertisers demand.

Our members want a safe space within which they can freely connect with one another, express themselves, share viewpoints, and explore culture. MySpace is a community much like the offline world. The best defense against those who would do us harm is to better understand the potential dangers and protect yourself as much as possible. If everyone applies real-world safety lessons online, whether on MySpace or elsewhere, the Internet really becomes a much safer place for all. When a crime does occur online, we need to ensure that we arm law enforcement with the appropriate knowledge, resources, and laws to identify, prosecute and bring these criminals to justice.

We first approach online safety by employing technologies that help protect teens from potential harm and inappropriate content and provide all members with tools they need to protect themselves. This is by no means an exhaustive list but here are some examples.

Profiles of users who are 14 and 15 are automatically set to private. We also now require that all users over the age of 18 must either know the email address or the first and last name of a member who is 14 or 15 to invite that member to become their friend. We have also recently implemented the privacy setting that is the default for 14- and 15-year-olds for all of our users. That allows our users to control the access and scope of their community.



MySpace reviews over 3 million images uploaded daily for content that violates our terms of use and we immediately remove any images that violate these terms. We also provide a link with each hosted image to allow users to report inappropriate content.

We recently developed and implemented proprietary technology to screen images on MySpace to assist us in quickly eradicating images that do not meet our standards. We also now provide a direct link to the cyber tip line to allow users to report incidents of child exploitation directly to the National Center. In addition, each page of our site contains a link to allow users to report inappropriate content and any other abuses that may occur on the site.

We are instituting new technologies that prevent users under the age of 18 from seeing advertising that is inappropriate for their age group. We have identified certain discussion groups that may contain material that is inappropriate for those under 18. Users under the age of 18 or who are not logged in cannot see or join these groups.

In addition to providing safety features and tools, education of users, parents and educators is a significant component of our efforts to foster a safer Internet. We believe that one of the best things that we can do for users is to teach them to protect themselves online just as they would in the real world and we are seeking help from parents, teachers, and others to help communicate this message. We include a link to clear common-sense safety tips on every page within our website. These tips are a must read as part of the registration process for every user under 18. We include a separate set of safety tips for parents and we emphasize that the most important thing that parents can do is to engage in a dialogue with their teens about Internet usage and we provide links to sites that help them do this. We also provide parents with step-by-step instructions on how to remove their teen's profile and include links to free software that enables them to limit access to the Internet including blocking MySpace entirely.

Finally, we view Internet safety as a collective priority and universal responsibility for all of us involved in the Internet--businesses, government, law enforcement, and users. We are constantly reaching out to those with expertise in the areas of child protection and Internet safety. Just last week as part of our effort to better educate ourselves on online safety, we participated in the National Center's dialogue on social networking to continue to explore ways to make the Internet safer for younger users through technology and education. In addition, we have a history of cooperation with law enforcement throughout the country and are frequently praised for our assistance. We have created a dedicated hotline staffed 24/7, and as the detective indicated, we have a law enforcement guide that has been widely disseminated to educate law

enforcement about MySpace and to instruct them how to process subpoena and information requests.

To continue to strengthen our existing partnerships and build new ones, we recently hired Hamu Niggam, our Chief Security Officer. Mr. Niggam has 16 years of safety and security experience including his work as a former Federal prosecutor specializing in crimes against children. He spent the last two days with 48 of the 50 Attorneys General at the annual NAG conference and focused on technology to make the Internet safer. We invited them to meet with us and our technical experts in the next 2 weeks to explore ways to implement viable age certification and we are currently coordinating schedules for that meeting.

In collaboration with the National Center and the Ad Council, we have engaged in the largest ever public service announcement campaign on Internet safety. These PSAs are featured repeatedly across all Fox properties, and I would like to show you a few of those PSAs right now.

[Video]

Mr. Chairman, members of the committee, thank you for your time and I look forward to answering any of your questions.

[The prepared statement of Michael Angus follows:]

PREPARED STATEMENT OF MICHAEL ANGUS, EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, FOX INTERACTIVE MEDIA, MYSPACE.COM

Mr. Chairman, Ranking Member Stupak and Members of the Committee, my name is Michael Angus and I am the general counsel of Fox Interactive Media, the parent company of MySpace. I want to thank you for inviting us here today to address concerns about Internet safety and to discuss how we can collectively protect younger users on the Internet.

Safety and security have been a priority for MySpace prior to the acquisition by Fox, and continue to remain a top priority at the highest levels of the company. We take seriously our responsibility to provide a safe and well-lit space for our members not only because it is the right thing to do, but because it also makes good business sense -- it is what our community and advertisers demand.

Our members want a safe space within which they can freely connect with one another, express themselves, share viewpoints, and explore culture. In that sense, as in many others, MySpace is a community much like the offline world. The best defense against those who would do us harm -- whether on the Internet or in any public place -- is to better understand the potential dangers and take active measures to protect yourself. If every person applies time-tested offline safety lessons to their online experiences, whether on MySpace or elsewhere, the Internet really becomes a much safer place for all. However, just as with any community, when a crime occurs online, we need to ensure that we arm law enforcement with the appropriate tools, knowledge, resources and consistent laws to identify, prosecute, and bring these criminals to justice.

As we have grown from a small site with a thousand users to now tens of millions, the challenges to meet safety concerns have grown. We are fully committed to meeting them head-on, and we continue to pursue a multi-pronged approach to Internet safety which

includes providing safety technologies, partnering with education and safety advocacy experts, and supporting law enforcement in their investigations.

#### **Online Safety Features:**

Safety online begins with safety features and safety tools for all of our users. We approach this challenge by employing safety technologies that help protect teens from potential harm and inappropriate content and provide all members with tools they need to help protect themselves.

We employ safety features specifically for younger teen users to help provide them with a safer environment. We have always set younger teen users' profiles to "private" by default, meaning that no one can view their profiles unless the younger teen user grants permission or overrides the default privacy setting. If that setting is overridden, the user will be presented with the safety tips yet again and will be required to confirm that they wish to change the profile from "private." And even if that default setting is changed, the profile is still only viewable by users under 18 and the "friends" of the user.

Just last week, we implemented additional safety features to help protect our younger teen users. In addition to our current features, we now require that all users over 18 must know either the email address or first and last name of the member in order to connect to a user who is 14 or 15. We will continue to identify further methods to provide a safer environment for our younger teen users.

Also, we continue to expand the safety tools we provide for all of our members. We now allow members of any age to set their profiles to private, allowing only friends within their private network to view their profile, such as information about personal interests and friends. Of course, we still recommend to users that, regardless of their privacy settings, they not post particular personal information that would help someone with bad motives to find them in the offline world. Just as you would not hand out your address or phone number to a group of strangers, we remind all users that information they make available over the Internet is broadly accessible.

We employ state-of-the-art technology to help protect our community and we are constantly seeking, testing, and implementing new safety products. We recently developed proprietary technology to screen images on MySpace to ensure that we are quickly eradicating images that do not meet our community standards. In addition, MySpace is providing further protections by instituting new technologies that prevent users under the age of 18 from seeing advertising that is inappropriate for their age group.

As safety technologies for the online space improve, we continue to explore further safety enhancements for our site to help protect members from inappropriate content and to provide members with the tools needed to protect themselves. Age verification, which at this stage is a form of identity verification, is one proposal that has been suggested to prevent predators from connecting with unsuspecting teens. We have met with numerous companies in search of a technology solution that would provide effective age

verification. While we have not found an effective solution to date, we continue to evaluate all available age verification technologies, as well as other technology approaches that will help to protect younger users.

Our users have helped us a great deal by reporting content that violates our policies. Partnering with the National Center for Missing and Exploited Children, we now provide a direct link to the CyberTipLine, which allows users to directly report images they suspect might be related in any way to child exploitation directly to the National Center, which then contacts the appropriate law enforcement agency to investigate.

#### **Education of Members, Parents and Educators:**

In addition to providing safety features and tools, educating users, parents, educators and school administrators about safe Internet usage is also a significant component of our efforts to foster a safer Internet. Our partners in safety have worked with us to provide education tools for all these audiences. We believe that one of the best things that we can do for users is to teach them to protect themselves online just as they would in the real world. And we are seeking help from parents, teachers and others to help communicate this message. We include a link to clear, common-sense safety tips on every page within our website. These tips are a must-read as part of the registration process for every user under 18, and we have separately communicated these tips to each user under 18 as a message in their Inbox. In addition, we include a separate set of safety tips for parents. We emphasize that the most important thing that parents can do is to engage in a dialogue with their teens about Internet usage, and we provide links to sites that help them do this. Also, we provide parents with step-by-step instructions on how to remove their teen's profile and include links to free software that enables them to limit access to the Internet, including blocking MySpace.

Additionally, we have created a Parents' Guide to further educate parents about safe Internet usage and how to talk to their teens about safe Internet usage, which will be distributed before the beginning of the coming school year. We are also in the process, working with major educational organizations, of creating an Educators' Guide and curriculum development tools to provide educators and school administrators with the tools to teach smart and safe web practices.

#### **Partnerships with Safety Experts, Government and Law Enforcement:**

Finally, we view Internet safety as a collective priority and universal responsibility for all of us involved in the Internet – businesses, government, law enforcement and users. The Internet has become a powerful, global means of distributing information and communicating. The issues we face as a social networking site are not new, but they have become more focused and concentrated, if for no other reasons than the advent of broadband and increased usage of the Internet as a communications tool. Because of the importance of these issues and the many different viewpoints on Internet safety and security, we have sought input from and forged relationships with a variety of groups to

address safety issues collectively. We believe that this will result in a safer Internet for everyone.

From our early relationship with Wired Safety to our close partnership with the National Center for Missing and Exploited Children (NCMEC), we are reaching out to those with expertise in areas of child protection and Internet safety. In collaboration with the NCMEC and the Ad Council, News Corporation (the parent company of Fox Interactive Media) and MySpace have engaged in the largest-ever Public Service Announcement (PSA) campaign on Internet safety. These PSAs are featured repeatedly across all Fox properties, including online, radio, print, network and cable channels. These PSAs can be viewed at: <http://www.adcouncil.org/default.aspx?id=56>.

Just last week, as part of our effort to better educate ourselves on online safety we participated in NCMEC's Dialogue on Social Networking. This was an effort by NCMEC to bring together safety experts to discuss the concerns associated with social networking sites and what steps could be taken to address Internet safety. We look at this event as a major step in our ongoing dialogue with experts to help guide us as we work through these important safety issues, implement more safety features, and engage in broader educational efforts.

In addition, we have a history of cooperation with law enforcement agencies throughout the country and are frequently praised for our assistance and cooperation. To assist law enforcement in their investigations, we have created a dedicated hotline that is staffed 24/7 and a Law Enforcement Guide that has been widely disseminated to educate law enforcement about MySpace and to instruct them on how to process subpoena and information requests relating to MySpace.

As you probably know, we have been in contact with numerous State Attorneys General and have been working with them to address safety concerns inherent in the Internet and in social networking. Many of our recent changes are the product of discussions with them as well as with this Subcommittee.

To continue to strengthen our existing partnerships and to build new ones, we recently hired Hemanshu Nigam as our Chief Security Officer. Mr. Nigam has sixteen years of safety and security experience, including his work as a former Federal prosecutor who specialized in crimes against children. He is currently presenting at the annual meeting of the National Association of Attorneys General to continue our ongoing safety dialogue.

#### **Good Things:**

Finally, I would like to take a moment to talk about the good that comes from social networking sites like MySpace. While our members are certainly connecting over new music, films, comedies, and other popular culture, they are also working to make the world a better place.

MySpace has nearly 18,000 groups dedicated to Government and Politics, more than 11,000 groups devoted to Non-Profit and Philanthropic activities, and 67,000 groups focused on Religion and Beliefs.

In the Chairman's and Congressman Burgess' home state of Texas, a doctor created Operation Helmet which is sending equipment upgrade kits to troops in Iraq and Afghanistan to provide additional protection to our troops on the front lines. Operation Helmet is spreading the word and raising money through their more than one thousand friends on MySpace, and has even received praise from Secretary of Defense Donald Rumsfeld.

In Congressman Pickering's home state of Mississippi, MySpace members were instrumental in lining up temporary guest housing for evacuees after Hurricane Katrina, and we are currently donating promotional support to a 501(c)3 that is rebuilding a Boys' and Girls' Club in Gulfport.

In Congressman Waxman's home state of California, the Surfrider Foundation is using MySpace to build a network of friends committed to keeping our oceans and beaches clean and safe.

Even candidates for Congress are using MySpace to educate voters about the issues, register constituents to vote, and ensure they have a way to get to the polls on Election Day.

All over the country, we are seeing good works happening through MySpace and through its users.

Mr. Chairman, I fully appreciate that we need to address the safety challenges posed by the Internet, and I look forward to answering your questions on that subject. Keeping the Internet safe is a top priority for us as well as a shared responsibility for all of us. That is why we are creating lasting partnerships with leading child safety organizations, law enforcement, and government agencies. It is why we are working hard to educate our members, parents and educators. And, it is why we are actively engaged in protecting our younger members through our policies and technology tools. The same rules that we as parents teach our teens about how to be safe in the real world must be applied online. I look forward to answering any questions that you or Members of the Committee may have.

Thank you.

### **About MySpace**

MySpace is a Social Networking community where users connect around shared interests – whether those interests are music, movies, religion, politics, or other popular culture. MySpace has developed and integrated features including: blogs, user profiles, music, games, affinity groups, forums, Instant Messaging, mail, film, and classifieds that facilitate this social interaction. Although most of these features can be found on other large portals, it is the tight and seamless integration of these tools that have lead to MySpace's dramatic growth.

MySpace users find old friends, plan their social lives, discover new music, promote charities, civic causes, and express themselves creatively on their MySpace pages. MySpace is a new communication mechanism for the Internet generation much like email, instant messaging, or mobile devices. It is also one of the fastest growing forms of entertainment on the web or elsewhere. Following are some key facts about MySpace:

- Over 85 million members
- 250,000 new registered users per day
- #2 ranked site on the Internet in terms of page views (comScore Media Metrix)
- 78% of the users on the site are 18 years of age or older (comScore Media Metrix)
- MySpace music includes more than 1mm bands who have created music profiles and uploaded music
- MySpace has also recently launched an independent Film Maker Community that allows aspiring filmmakers to upload their short films to be seen and discovered by millions of people in an environment that previously didn't exist

### **Chief Safety and Security Officer**

Fox Interactive Media (MySpace's parent company) recently hired Hemashu Nigam as Chief Security Officer. Mr. Nigam formerly led child safe computing at the Microsoft Corporation. Prior to that, he was a trial attorney in the United States Department of Justice, Criminal Division, specializing in child pornography, child predator, and child online protection issues. Mr. Nigam oversees the initiatives described below.

### **MySpace's Content Policy**

MySpace's current procedures include providing a link to: (1) the Terms of Use, (2) the Privacy Policy, (3) Safety Tips, and (4) a link to "Contact My Space," which presents an easy way for users to report "abuse" on the site including "underage users" and "inappropriate content." The MySpace Photo Policy, which is available via a link from the photo upload section, prohibits posting photos that contain "nudity, pornography and sexually explicit images." MySpace removes from the site any member photos it discovers that violate the Terms of Use or the Photo policy, and provides a link for users to report offending photos. MySpace is diligent in reviewing its site for inappropriate content, reviewing each image and photo that is uploaded to the MySpace server on a daily basis for compliance with the Terms of Use and Photo Policy. In addition, we rely on our users to tell us about content that violates these policies. At the bottom of each profile page there is a link to "Report Inappropriate Content," as well as "Contact MySpace" links throughout the site, where users can report any profile or other area of the site, respectively, with questionable content. MySpace personnel investigate any reported profile, and if an image on the website violates the Terms of Use, the Photo Policy or is otherwise deemed inappropriate, the image and possibly the entire profile will be deleted. The MySpace staff will, as warranted by the circumstances, additionally investigate the user's friends to look for patterns of violations and more inappropriate content.

The majority of inappropriate images on MySpace is not hosted by MySpace, but rather are linked images. MySpace is committed to working with the two largest photo hosting sites to set joint standards for appropriate materials on the MySpace site and has accelerated its discussions with these sites. If these photo hosting services do not meet these standards, MySpace is prepared to terminate their access to MySpace. MySpace is also investigating software that enhances its ability to monitor pornography that is served into the site by third parties.

There may be MySpace "groups" that engage in adult discussions that are appropriate for adults but not for minors. MySpace has designated these groups as "adult only." These groups would not be listed on



the Groups List available on MySpace, and non-registrants and registered users under 18 would not be able to access or join adult-only groups.

If MySpace discovers any child pornography, it promptly reports it to federal law enforcement. MySpace will lock the profile so that the user will be unable to make any changes or even access the profile. MySpace submits the images and information to law enforcement so that the authorities can identify the profile on the MySpace system through a special login on the CyberTipline at the National Center for Missing and Exploited Children.

MySpace also now allows its users to link directly to the CyberTipline and report any incidents of child exploitation directly to the National Center for Missing and Exploited Children.

#### **How MySpace Works with Law Enforcement**

MySpace is constantly engaged with local police and investigators regarding user safety. MySpace has been praised for its cooperation with local, state and federal law enforcement agencies. Since its creation, MySpace has met with law enforcement officials throughout the country to solicit their viewpoints on how MySpace can enhance its cooperation with law enforcement and increase user security. MySpace has created streamlined procedures for law enforcement to submit subpoenas and other legal process to MySpace to obtain critical data that can be used to find and prosecute criminals. MySpace currently has a Law Enforcement Guide that instructs law enforcement agencies how to work with MySpace regarding subpoenas and requests for information, which has been broadly distributed to law enforcement groups around the country. MySpace is also creating a curriculum for law enforcement to track suspicious behavior on the Internet, and educate the public.

#### **Identifying Underage members**

MySpace is very concerned about underage users on the site. The registration page requires prospective members to enter their exact birth date, and individuals who enter a date that does not meet the requisite age (14 or older) are not permitted to register. Once a user enters an underage date, MySpace places a session cookie on their computer to prevent another registration attempt during the same browser session, i.e. preventing "back-buttoning."

If an individual is underage but enters a false birth date and is able to register for the website, there are still mechanisms in place to discover such underage users. MySpace has developed a search methodology to seek out such individuals, using over 1,000 search terms to alert the staff to a possible underage user on the site. The site is continually scanned for

such terms, and the database of search terms is constantly updated to reflect changes in user behavior and terminology. All profiles that are identified by these scans as potentially belonging to an underage user are then individually reviewed by MySpace personnel. In addition, the MySpace customer support team reviews profiles on the site to identify possible underage users that have been reported by MySpace members and parents to MySpace. Whenever an underage user is discovered, the profile is promptly deleted. Over 2,000 underage users are deleted each day as a result of the MySpace scanning process, and a comparable number are deleted daily based on reports from parents and other MySpace users.

### **Protecting Our Younger Members**

In the event a registered user is between fourteen and eighteen years old, MySpace maintains extra safety mechanisms to protect them. MySpace has created a special set of “Safety Tips” for younger members that highlights the most important lessons for Internet safety (they shouldn’t post anything they wouldn’t want the world to know; they should exercise caution when communicating with people they don’t know; and they should avoid meeting strangers off line but, if they must, they should bring a friend or trusted adult). These tips appear on the MySpace registration page for any user who indicates he/she is under 18, and anyone under 18 must actually indicate that they’ve read these tips before they can register. The tips have also been posted in the “mail” area for existing members of MySpace who are under 18. In addition, MySpace will communicate safety tips and reminders periodically to under-18 users.

Profiles of users who are 14 and 15 are automatically set to be private. This means that only the user’s “friends” (that is, individuals that the user has affirmatively chosen to add to his or her “friends” list) will be able to view the profile. Additionally, only the user’s friends will be able to send email messages or IM messages to the user, or add the user to a blog list. If a user chooses to override this setting, the user will see specific safety tips about the disclosure of personally identifiable information and will be required to confirm changing this setting. Even if the default privacy setting is overridden, the profile is only viewable by the user’s friends other users under 18. These privacy features are intended to prevent members who are 18 years of age or over from viewing a profile or sending an unsolicited message to users who are under 16.

### **Education of members, parents and educators**

MySpace has recently revised its Safety Tips for parents and users to make them more clear and concise. Links to these Tips appear at the bottom of every page of the site. The Safety Tips for users provide guidelines on how to use MySpace safely. Tips for parents are designed to educate the parents about the site and how to help their children to make safe decisions about using online communities. It also encourages parents to talk to their kids about how they communicate with others and represent themselves on MySpace. Additionally, it provides parents with step-by-step instructions to remove their child's profile and links to free software to enable parents to monitor or block their child's use of the Internet, including blocking MySpace.

MySpace is creating a curriculum for PTAs, schools, church or civic groups, and local organizations to educate teens and families on Internet safety.

### **Education Partnerships**

MySpace is planning a series of outreach programs to emphasize online safety in the age of social networking. MySpace exploring outreach programs individually and hopefully in conjunction with other online community sites.

- News Corporation and MySpace have engaged in the largest Public Service Announcement (PSA) campaigns on Internet safety with the National Center for Missing and Exploited Children (NCMEC).
- MySpace is developing a School Administrators Guide to provide educators with information about how to work with MySpace, and MySpace has met with many educational organizations to seek their input.
- MySpace is developing celebrity-based multimedia PSA campaigns on Internet safety via multiple media outlets in addition to online PSAs.
- MySpace is exploring partnerships to develop materials for teachers and law enforcement to perform safety education in schools.
- MySpace is exploring a forum to educate parents, give them a voice and connect them around the issue of internet safety.

- MySpace is working with the NCMEC to streamline reporting procedures for child pornography and other child safety issues, to set standards for communication between social websites and NCMEC and share knowledge among and between participants in the industry and the relevant organizations.



News Corporation

[Filmed Entertainment](#)
[Television](#)
[Cable](#)
[Direct Broadcast Satellite Television](#)
[Magazines & Inserts](#)
[Newspapers](#)
[Books](#)
[Other](#)

[Corporate Governance](#)  
[Press Releases](#)  
[Investor & Financial](#)  
[Executive & Contacts](#)  
[Careers](#)

## press releases

### MYSPACE NAMES HEMANSHU NIGAM CHIEF SECURITY OFFICER

Nigam to Oversee All Safety, Education, Privacy and Law Enforcement Programs for MySpace and other Fox Interactive Media Properties

**SANTA MONICA, April 11, 2006** - Fox Interactive Media (FIM), parent of MySpace.com, has appointed industry veteran Hemanshu (Hemu) Nigam to oversee safety, education and privacy programs and law enforcement affairs for MySpace, as well as the growing network of FIM properties. Nigam, who currently serves as Director of Consumer Security Outreach & Child Safe Computing at the Microsoft Corporation, brings more than 15 years of experience in online safety for private industry and law enforcement, including serving as a Federal prosecutor against Internet child exploitation for the US Department of Justice, an advisor to a Congressional commission on online child safety, and an advisor to the White House on cyberstalking. Nigam's appointment is effective May 1, 2006.

"Hemu is a proven leader in online safety and security. We are fortunate to have him join MySpace, help us educate the public and protect our members' safety and privacy," said Chris DeWolfe, CEO of MySpace. "MySpace has always been committed to an industry leading role in internet safety and will continue to partner with all stakeholders including parents, educators, law enforcement and safety groups."

"Fox Interactive Media and its network of properties will greatly benefit from Hemu's experience, stature among law enforcement and private industry leaders, and strategic vision," said Ross Levinsohn, President of Fox Interactive Media. "We look forward to working with Hemu as we continue in our commitment to provide a leadership role in developing industry standards that safeguard our growing community of members."

Nigam's role at Microsoft has been to lead the team within Microsoft's Security Technology Unit responsible for driving consumer security outreach and child safe computing strategies. Nigam oversees outreach and partnership development with government agencies and non-governmental organizations (NGOs) involved in online consumer safety and security. He led the cross-company child safety initiative launched to build a holistic approach to child safe computing throughout Microsoft products, services and programs. Nigam also served as a spokesperson on virus, hacking and spam enforcement outreach, and on child online protection and law enforcement outreach.

Prior to joining Microsoft, Nigam served as vice president of Worldwide Internet Enforcement at the Motion Picture Association of America. There he built and oversaw the global strategy to combat online motion picture piracy for the seven major Hollywood studios.

In his prior role, he was a trial attorney in the United States Department of Justice, Criminal Division, in Washington, D.C. where he specialized in child pornography, child predator and child trafficking and computer crime cases nationwide. Nigam also served on the Vice President's Committee on CyberStalking and was a legal advisor to the COPA Commission (created by the Child Online Protection Act, the landmark 1998 piece of legislation defending children's safety online, to advise Congress). He was also the law enforcement liaison to ISPs and filtering technology companies on child online protection issues.

The appointment demonstrates MySpace's ongoing commitment to protecting the safety of its more than 68 million members. Since the inception of the site, the company has devoted extensive resources towards these important issues and has created a deep arsenal of programs and services deployed on the site to maintain the security of its members including:

- Limiting use of the site to members who are at least 14 years of age and providing special protections to members who are under 16 so their personal information cannot be accessed by persons they do not know.
- Requiring all new members under 18 years of age to review safety tips prior to registration.
- Deleting profiles of under-age members. Since the inception of the site, the company has deleted

more than 250,000 underage profiles.

- Reviewing every image hosted directly to the site – more than 2 million every day.
- Members often link to images hosted on other sites from their MySpace pages and MySpace is working with the largest image hosting companies on the web to ensure that these companies are monitoring the photos and adhering to MySpace's policies.
- Limiting access to certain discussion groups with adult themes to members 18 years of age and over.
- Providing parents links to free filtering software to guide their child's Internet activities and access.
- Providing mechanisms, including links next to every photo hosted on the site, so members can report inappropriate content to MySpace.
- Working with hundreds of law enforcement agencies at the federal, state, and local levels to address potential issues quickly and effectively.
- Offering revised safety information and tips from every page of the website for both users and parents.
- Partnering with the National Center for Missing and Exploited Children and the Advertising Council, as announced recently, to promote online safety through a series of national public service advertisements – the largest single campaign ever run on behalf of the National Center for Missing and Exploited Children.

#### About MySpace.com

MySpace is the premier lifestyle portal for connecting with friends and discovering popular culture. By integrating web profiles, blogs, instant messaging, e-mail, music streaming, music videos, photo galleries, classified listings, events, groups, college communities and member forums, MySpace has created a connected community. As the second ranked web domain in terms of page views\*, MySpace.com is the most widely-used and highly regarded site of its kind. With more than 70 million members, MySpace is committed to providing the highest quality member experience and will continue to innovate with new features that allow its members to express their creativity and share their lives, both online and off.

\* Among the top 2000 domains. comScore Media Metrix, March 2006. For more information on comScore Networks, please go to <http://www.comscore.com>.

#### About Fox Interactive Media

With the third largest reach of any Internet company, Fox Interactive Media (FIM) is building an integrated network of sites that offer its more than 70 million worldwide members socially rich media experiences centered on entertainment, news, information and self-expression. The company's network includes assets from News Corp. divisions, including the highly trafficked Foxsports.com, Americanidol.com and Fox.com. FIM also owns and operates such category leaders as MySpace, the number one social networking site on the Web; IGN, a leading gaming and entertainment site; Scout.com, a dynamic collegiate and pro sports network of property; AskMen, a leading men's lifestyle site, and Rotten Tomatoes, the premier destination for movie-goers, among others.

# # #

Contacts:  
Matthew Grossman for MySpace.com  
[matthew.grossman@edelman.com](mailto:matthew.grossman@edelman.com)  
(323) 202-1061

Julie Henderson for Fox Interactive Media  
[Julie.henderson@fox.com](mailto:Julie.henderson@fox.com)  
(310) 969-7141




[Home](#) > News Detail

## News Detail

### **National Center for Missing and Exploited Children, The Ad Council and MySpace Partner to Promote Online Safety**

April 10, 2006

*Public Service Advertisements to Run On News Corporation's Outlets Including Television, The Internet, and Newspapers*

Los Angeles, CA, – April 10 2006 – The National Center for Missing & Exploited Children® (NCMEC), the Advertising Council and News Corporation, parent company of Fox Interactive Media and MySpace, announced today a joint effort to promote online safety through the deployment of a series of national public service advertisements (PSAs). The PSAs, part of an ongoing Ad Council campaign, will begin running today through News Corporation's broad network of distribution channels, and are designed to raise awareness about Internet safety and education.

The campaign is part of an ongoing, industry-wide effort led by MySpace, Fox Interactive Media and News Corporation to work with leading advocacy organizations to develop safety curriculum and educate the public on online safety.

"Fox Interactive Media now has the third largest reach of any Internet company and from the top down, News Corp is committed to making the Internet as safe as possible. We're delighted to be working with the National Center for Missing & Exploited Children and the Ad Council on this important awareness initiative," said Peter Chernin, President and Chief Operating Officer of News Corporation. "We will be leveraging the full power of News Corp's broad distribution channels to get their message out and remain deeply committed to promoting online safety."

"We know the Internet holds tremendous potential for our nation's youth," said Ernie Allen, President and CEO of NCMEC. "We are pleased to be partnering with News Corp and MySpace to extend the reach of our ad campaign so that we can educate additional parents, guardians, and teens about how to prevent online victimization so our children may have safer experiences online."

"We are grateful to News Corporation for their generous commitment of donated advertising time and space to this important campaign. Their support in media frequented by our target audience will go a long way to getting this important message out to teens and their parents," said Peggy Conlon, President and CEO of the Advertising Council.

"Since its inception MySpace has worked with law enforcement to aid in the protection of teens and help find runaways," said Chris DeWolfe, CEO of MySpace. "So, this partnership makes a lot of sense on many levels given NCMEC's position as the premier organization in helping find and protect children."

Sponsored by NCMEC and created pro bono by ad agency Merkley + Partners, the PSAs are designed to educate parents and guardians about measures they can take to better protect their children online, and to educate teens on how to be smart and maintain safe online relationships. The PSAs direct parents, guardians, and teens to visit [www.cybertipline.com](http://www.cybertipline.com) to learn about safe and responsible use of the Internet, as well as how to report threats.

The PSAs will air on primetime on FOX, and across Fox Interactive Media's network of websites including MySpace, FoxSports.com, IGN.com, Fox.com, AmericanIdol.com, Rotten Tomatoes and AskMen. The PSAs will also air on the 28 Fox Networks Group broadcast, cable and satellite services. Fox broadcast and cable networks running the campaign will include FOX, FX, National Geographic channel, Fox Movie Channel, Fox Reality, FUEL TV, FSN, SPEED, Fox College Sports Atlantic, Fox College Sports Central, Fox College Sports Pacific, Fox Soccer Channel and (in Spanish) on Fox Sports en Espanol. All Fox-owned-and-operated regional sports networks will likewise televise the PSAs. Additionally, Fox All Access radio and the New York Post will run the campaign.

#### **About the National Center for Missing & Exploited Children (NCMEC)**

NCMEC is a 501(c)(3) nonprofit organization that works in cooperation with the U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention. NCMEC's congressionally mandated CyberTipline, a reporting mechanism for child sexual exploitation, has handled more than 365,600 leads. Since 1984, NCMEC has assisted law enforcement with more than 117,100 missing child cases, resulting in the recovery of more than 99,500 children. For more information about NCMEC, call its toll-free, 24-hour hotline at 1-800-THE-LOST or visit its web site at [www.missingkids.com](http://www.missingkids.com).

#### **About The Advertising Council**

The Ad Council is a private, non-profit organization with a rich history of marshalling volunteer talent from the advertising and media industries to deliver critical messages to the American public. Having produced literally thousands of PSA campaigns addressing the most pressing social issues of the day, the Ad Council has effected, and continues to affect, tremendous positive change by raising awareness, inspiring action and saving lives.

#### **About MySpace.com**

MySpace is the premier lifestyle portal for connecting with friends and discovering popular culture. By integrating web profiles, blogs, instant messaging, e-mail, music streaming, music videos, photo galleries, classified listings, events, groups, college communities and user forums, MySpace has created a connected community. As the second ranked web domain in terms of page views\*, MySpace.com is the most widely-used and highly regarded site of its kind. With more than 65 million members, MySpace is committed to providing the highest quality user experience and will continue to innovate with new features that allow its users to express their creativity and share their lives, both online and off.

\* Among the top 2000 domains. comScore Media Metrix, February 2006. For more information on comScore Networks, please go to [www.comscore.com](http://www.comscore.com).

**News Corporation** (NYSE: NWS, NWS.A; ASX: NWS, NWSLV) had total assets as of December 31, 2005 of approximately US \$55 billion and total annual revenues of approximately US \$24 billion. News Corporation is a diversified international media and entertainment company with operations in eight industry segments: filmed entertainment; television; cable network programming; direct broadcast satellite television; magazines and inserts; newspapers; book publishing; and other. The activities of News Corporation are conducted principally in the United States, Continental Europe, the United Kingdom, Australia, Asia and the Pacific Basin.

#### **MEDIA CONTACTS:**

##### **Fox Interactive Media/News Corporation:**

Julie Henderson  
310-969-7141  
[julie.henderson@fox.com](mailto:julie.henderson@fox.com)

##### **MySpace:**

Dani Dudeck at Edelman  
323-202-1890  
[dani.dudeck@edelman.com](mailto:dani.dudeck@edelman.com)



**NCMEC Communications Department:**  
703-837-6111

[Return to Previous Page](#)

**FOR IMMEDIATE RELEASE****MYSPACE EXPANDS SAFETY AND SECURITY PRODUCT  
FEATURES TO HEIGHTEN ONLINE SAFETY FOR MEMBERS****Leading Social Networking Site to Increase Protection for 14-15 Year Old  
Members; Adds Ability for Members to Set Profile to Private**

LOS ANGELES—June 21, 2006—MySpace.com, the leading social networking and lifestyle portal, announced today new safety and security features designed to offer increased safety to its growing community of members. These additional safety features include heightened security for 14–15 year old members, new options for privacy settings for all members, and restrictions on ad placements to younger users.

Directing all MySpace's safety and security policies is newly appointed MySpace Chief Security Officer, Hemanshu Nigam, a former Federal prosecutor against Internet child exploitation for the U.S. Department of Justice.

"With social networking becoming a mainstream platform for millions of people to connect with one another and express themselves, MySpace is committed to innovating new product features to heighten online safety, particularly in the area of 14 to 15 year olds," said Nigam. "In addition to technology innovation, MySpace remains dedicated to a multi-pronged approach that also involves education and collaboration with law enforcement, teachers, parents and members."

MySpace's new enhanced safety features include:

- **Heightened Security Settings for 14 -15 Year Olds:** Furthering efforts to create a well-lit place for teens to connect and communicate online, MySpace will now protect 14 and 15 year olds from contact from strangers, who are over 18 years old. This new feature requires all 18+ year old members to know either the email address or first and last name of members who are under 16 years old to connect.
- **Full Privacy Settings for All Members:** MySpace members of any age have the option to set their profiles to private, allowing only friends within their private network to view detailed information such as personal interests and friends. In addition, MySpace members have the option to set their profile to restrict contact to members within their own age group.
- **Age Appropriate Ad Placements:** In an additional move to safeguard and enhance members' experience, MySpace is improving advertising targeting throughout the site based on age appropriateness. MySpace will engage in targeted online ad placements in order to promote safe Internet behavior.

"We know that children can benefit greatly from being online," said Ernie Allen, President and CEO of the National Center for Missing & Exploited Children (NCMEC).

“We commend MySpace for adding new safety and security features that will help provide protection to their youngest members, so they can have a safer online experience.”

The efforts announced today are part of a broad effort at MySpace to help protect the privacy of community members and provide a safer environment for users to connect online. These safety features complement MySpace’s ongoing safety campaign created to promote safer Internet practices. Earlier this year, MySpace in partnership with NCMEC and the Advertising Council deployed a series of national public service advertisements (PSAs). The PSAs, part of an ongoing Ad Council campaign, are running on News Corporation’s broad network of distribution channels, and are designed to raise awareness about Internet safety and education.

# # #

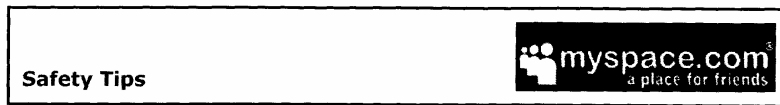
#### About MySpace.com

MySpace, a unit of Fox Interactive Media Inc., is the premier lifestyle portal for connecting with friends and discovering popular culture. By integrating web profiles, blogs, instant messaging, e-mail, music streaming, music videos, photo galleries, classified listings, events, groups, college communities and member forums, MySpace has created a connected community. As the second ranked web domain in terms of page views\*, MySpace.com is the most widely-used and highly regarded site of its kind. With more than 80 million member profiles, MySpace is committed to providing the highest quality member experience and will continue to innovate with new features that allow its members to express their creativity and share their lives, both online and off.

\*Among the top 2000 domains comScore Media Metrix, April 2006. For more information on comScore Networks, please go to <http://www.comscore.com>.

#### Contacts:

Matthew Grossman for MySpace.com  
(323) 202-1061  
[matthew.grossman@edelman.com](mailto:matthew.grossman@edelman.com)

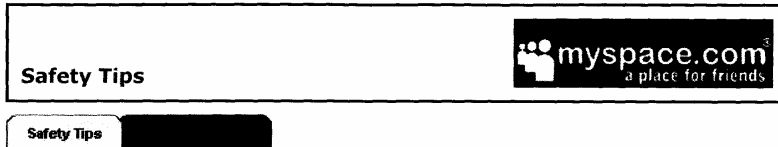
**Tips for Parents**

MySpace makes it easy to express yourself, connect with friends and make new ones, but please remember that what you post publicly could embarrass you or expose you to danger. Here are some common sense guidelines that you should follow when using MySpace:

- **Don't forget that your profile and MySpace forums are public spaces.** Don't post anything you wouldn't want the world to know (e.g., your phone number, address, IM screen name, or specific whereabouts). Avoid posting anything that would make it easy for a stranger to find you, such as where you hang out every day after school.
- **People aren't always who they say they are. Be careful about adding strangers to your friends list.** It's fun to connect with new MySpace friends from all over the world, but avoid meeting people in person whom you do not fully know. If you must meet someone, do it in a public place and bring a friend or trusted adult.
- **Harassment, hate speech and inappropriate content should be reported.** If you feel someone's behavior is inappropriate, react. Talk with a trusted adult, or report it to MySpace or the authorities.
- **Don't post anything that would embarrass you later.** Think twice before posting a photo or info you wouldn't want your parents or boss to see!
- **Don't mislead people into thinking that you're older or younger.** If you lie about your age, MySpace will delete your profile.

**To learn more please visit these other resources:**

- [Netsmartz.org](http://Netsmartz.org)
- [SafeTeens.com](http://SafeTeens.com)
- [WebWiseKids.org](http://WebWiseKids.org)



For teens, MySpace is a popular online hangout because the site makes it easy for them to express themselves and keep in touch with their friends.

As a parent, please consider the following guidelines to help your children make safe decisions about using online communities.

- **Talk to your kids about why they use MySpace, how they communicate with others and how they represent themselves on MySpace.**
- **Kids shouldn't lie about how old they are. MySpace members must be 14 years of age or older.** We take extra precautions to protect our younger members and we are not able to do so if they do not identify themselves as such. MySpace will delete users whom we find to be younger than 14, or those misrepresenting their age.
- **MySpace is a public space.** Members shouldn't post anything they wouldn't want the world to know (e.g., phone number, address, IM screen name, or specific whereabouts). Tell your children they should avoid posting anything that would make it easy for a stranger to find them, such as their local hangouts.
- **Remind them not to post anything that could embarrass them later or expose them to danger.** Although MySpace is public, teens sometimes think that adults can't see what they post. Tell them that they shouldn't post photos or info they wouldn't want adults to see.
- **People aren't always who they say they are. Ask your children to be careful about adding strangers to their friends list.** It's fun to connect with new MySpace friends from all over the world, but members should be cautious when communicating with people they don't know. They should talk to you if they want to meet an online friend in person, and if you think it's safe, any meeting should take place in public and with friends or a trusted adult present.
- **Harassment, hate speech and inappropriate content should be reported.** If your kids encounter inappropriate behavior, let them know that they can let you know, or they should report it to MySpace or the authorities.

[Click Here](#) to remove your [child's profile](#) from MySpace

For more information on Monitoring software, please visit:

- [Software4parents.com](#)
- [k9webprotection.com](#)

To learn more please visit these other resources:

- [Netsmartz.org](#)
- [WiredSafety.org](#)
- [The Child Safety Network](#)
- [GetNetWise.org](#)
- [SafeTeens.com](#)

**Terms & Conditions****MySpace.com Terms of Use Agreement****June 15, 2006**

MySpace.com is a social networking service that allows Members to create unique personal profiles online in order to find and communicate with old and new friends. The services offered by MySpace.com ("Myspace.com" or "we") include the MySpace.com website (the "MySpace Website"), the MySpace.com Internet messaging service, and any other features, content, or applications offered from time to time by MySpace.com in connection with the MySpace Website (collectively, the "MySpace Services"). The MySpace Services are hosted in the U.S.

This Terms of Use Agreement ("Agreement") sets forth the legally binding terms for your use of the MySpace Services. By using the MySpace Services, you agree to be bound by this Agreement, whether you are a "Visitor" (which means that you simply browse the MySpace Website) or you are a "Member" (which means that you have registered with Myspace.com). The term "User" refers to a Visitor or a Member. You are only authorized to use the MySpace Services (regardless of whether your access or use is intended) if you agree to abide by all applicable laws and to this Agreement. Please read this Agreement carefully and save it. If you do not agree with it, you should leave the MySpace Website and discontinue use of the MySpace Services immediately. If you wish to become a Member, communicate with other Members and make use of the MySpace Services, you must read this Agreement and indicate your acceptance during the Registration process.

This Agreement includes MySpace.com's policy for acceptable use of the MySpace Services and Content posted on the MySpace Website, your rights, obligations and restrictions regarding your use of the MySpace Services and MySpace.com's Privacy Policy. In order to participate in certain MySpace Services, you may be notified that you are required to download software or content and/or agree to additional terms and conditions. Unless otherwise provided by the additional terms and conditions applicable to the MySpace Services in which you choose to participate, those additional terms are hereby incorporated into this Agreement. You may receive a copy of this Agreement by emailing us at: [privacy@MySpace.com](mailto:privacy@MySpace.com), Subject: Terms of Use Agreement.

MySpace.com may modify this Agreement from time to time and such modification shall be effective upon posting by MySpace.com on the MySpace Website. You agree to be bound to any changes to this Agreement when you use the MySpace Services after any such modification is posted. It is therefore important that you review this Agreement regularly to ensure you are updated as to any changes.

Please choose carefully the information you post on MySpace.com and that you provide to other Users. Your MySpace.com profile may not include the following items: telephone numbers, street addresses, last names, and any photographs containing nudity, or obscene, lewd, excessively violent, harassing, sexually explicit or otherwise objectionable subject matter. Despite this prohibition, information provided by other

MySpace.com Members (for instance, in their Profile) may contain inaccurate, inappropriate, offensive or sexually explicit material, products or services, and MySpace.com assumes no responsibility or liability for this material. If you become aware of misuse of the MySpace Services by any person, please contact [MySpace](#) or click on the "Report Inappropriate Content" link at the bottom of any MySpace.com page.

MySpace.com reserves the right, in its sole discretion, to reject, refuse to post or remove any posting (including private messages) by you, or to restrict, suspend, or terminate your access to all or any part of the MySpace Services at any time, for any or no reason, with or without prior notice, and without liability.

1. **Eligibility.** Use of and Membership in the MySpace Services is void where prohibited. By using the MySpace Services, you represent and warrant that (a) all registration information you submit is truthful and accurate; (b) you will maintain the accuracy of such information; (c) you are 14 years of age or older; and (d) your use of the MySpace Services does not violate any applicable law or regulation. Your profile may be deleted and your Membership may be terminated without warning, if we believe that you are under 14 years of age.
2. **Term.** This Agreement shall remain in full force and effect while you use the MySpace Services or are a Member. You may terminate your Membership at any time, for any reason, by following the instructions on the Member's Account Settings page. MySpace.com may terminate your Membership at any time, without warning. Even after Membership is terminated, this Agreement will remain in effect, including sections 5-17.
3. **Fees.** You acknowledge that MySpace.com reserves the right to charge for the MySpace Services and to change its fees from time to time in its discretion. If MySpace.com terminates your Membership because you have breached the Agreement, you shall not be entitled to the refund of any unused portion of subscription fees.
4. **Password.** When you sign up to become a Member, you will also be asked to choose a password. You are entirely responsible for maintaining the confidentiality of your password. You agree not to use the account, username, or password of another Member at any time or to disclose your password to any third party. You agree to notify MySpace.com immediately if you suspect any unauthorized use of your account or access to your password. You are solely responsible for any and all use of your account.
5. **Non-commercial Use by Members.** The MySpace Services are for the personal use of Members only and may not be used in connection with any commercial endeavors except those that are specifically endorsed or approved by MySpace.com. Illegal and/or unauthorized use of the MySpace Services, including collecting usernames and/or email addresses of Members by electronic or other means for the purpose of sending unsolicited email or unauthorized framing of or linking to the MySpace Website is prohibited. Commercial advertisements, affiliate links, and other forms of solicitation may be removed from Member profiles without notice and may result in termination of Membership privileges. Appropriate legal action will be taken for any illegal or unauthorized use of the MySpace Services.
6. **Proprietary Rights in Content on MySpace.com.**



1. MySpace.com does not claim any ownership rights in the text, files, images, photos, video, sounds, musical works, works of authorship, or any other materials (collectively, "Content") that you post to the MySpace Services. After posting your Content to the MySpace Services, you continue to retain all ownership rights in such Content, and you continue to have the right to use your Content in any way you choose. By displaying or publishing ("posting") any Content on or through the MySpace Services, you hereby grant to MySpace.com a limited license to use, modify, publicly perform, publicly display, reproduce, and distribute such Content solely on and through the MySpace Services.

Without this license, MySpace.com would be unable to provide the MySpace Services. For example, without the right to modify Member Content, MySpace.com would not be able to digitally compress music files that Members submit or otherwise format Content to satisfy technical requirements, and without the right to publicly perform Member Content, MySpace.com could not allow Users to listen to music posted by Members. The license you grant to MySpace.com is non-exclusive (meaning you are free to license your Content to anyone else in addition to MySpace.com), fully-paid and royalty-free (meaning that MySpace.com is not required to pay you for the use on the MySpace Services of the Content that you post), sublicensable (so that MySpace.com is able to use its affiliates and subcontractors such as Internet content delivery networks to provide the MySpace Services), and worldwide (because the Internet and the MySpace Services are global in reach). This license will terminate at the time you remove your Content from the MySpace Services. The license does not grant MySpace.com the right to sell your Content, nor does the license grant MySpace.com the right to distribute your Content outside of the MySpace Services.

2. You represent and warrant that: (i) you own the Content posted by you on or through the MySpace Services or otherwise have the right to grant the license set forth in this section, and (ii) the posting of your Content on or through the MySpace Services does not violate the privacy rights, publicity rights, copyrights, contract rights or any other rights of any person. You agree to pay for all royalties, fees, and any other monies owing any person by reason of any Content posted by you to or through the MySpace Services.
3. The MySpace Services contain Content of MySpace.com ("MySpace.com Content"). MySpace.com Content is protected by copyright, trademark, patent, trade secret and other laws, and MySpace.com owns and retains all rights in the MySpace.com Content and the MySpace Services. MySpace.com hereby grants you a limited, revocable, nonsublicensable license to reproduce and display the MySpace.com Content (excluding any software code) solely for your personal use in connection with viewing the MySpace Website and using the MySpace Services.
4. The MySpace Services contain Content of Users and other MySpace.com licensors. Except for Content posted by you, you may not copy, modify, translate, publish, broadcast, transmit, distribute, perform, display, or sell any Content appearing on or through the MySpace Services.

**7. Content Posted.**

1. MySpace.com may delete any Content that in the sole judgment of MySpace.com violates this Agreement or which may be offensive, illegal or violate the rights, harm, or threaten the safety of any person. MySpace.com assumes no responsibility for monitoring the MySpace Services for inappropriate Content or conduct. If at any time MySpace.com chooses, in its sole discretion, to monitor the MySpace Services, MySpace.com nonetheless assumes no responsibility for the Content, no obligation to modify or remove any inappropriate Content, and no responsibility for the conduct of the User submitting any such Content.
2. You are solely responsible for the Content that you post on or through any of the MySpace Services, and any material or information that you transmit to other Members and for your interactions with other Users. MySpace.com does not endorse and has no control over the Content. Content is not necessarily reviewed by MySpace.com prior to posting and does not necessarily reflect the opinions or policies of MySpace.com. MySpace.com makes no warranties, express or implied, as to the Content or to the accuracy and reliability of the Content or any material or information that you transmit to other Members.

**8. Content/Activity Prohibited.** The following is a partial list of the kind of Content that is illegal or prohibited to post on or through the MySpace Services. MySpace.com reserves the right to investigate and take appropriate legal action against anyone who, in MySpace.com's sole discretion, violates this provision, including without limitation, removing the offending communication from the MySpace Services and terminating the Membership of such violators. Prohibited Content includes, but is not limited to Content that, in the sole discretion of MySpace.com:

1. is patently offensive and promotes racism, bigotry, hatred or physical harm of any kind against any group or individual;
2. harasses or advocates harassment of another person;
3. exploits people in a sexual or violent manner;
4. contains nudity, violence, or offensive subject matter or contains a link to an adult website;
5. solicits personal information from anyone under 18;
6. provides any telephone numbers, street addresses, last names, URLs or email addresses;
7. promotes information that you know is false or misleading or promotes illegal activities or conduct that is abusive, threatening, obscene, defamatory or libelous;
8. promotes an illegal or unauthorized copy of another person's copyrighted work, such as providing pirated computer programs or links to them, providing information to circumvent manufacture-installed copy-protect devices, or providing pirated music or links to pirated music files;
9. involves the transmission of "junk mail," "chain letters," or unsolicited mass

mailing, instant messaging, "spimming," or "spamming";

10. contains restricted or password only access pages or hidden pages or images (those not linked to or from another accessible page);
11. furthers or promotes any criminal activity or enterprise or provides instructional information about illegal activities including, but not limited to making or buying illegal weapons, violating someone's privacy, or providing or creating computer viruses;
12. solicits passwords or personal identifying information for commercial or unlawful purposes from other Users;
13. involves commercial activities and/or sales without our prior written consent such as contests, sweepstakes, barter, advertising, or pyramid schemes;
14. includes a photograph of another person that you have posted without that person's consent; or
15. for band and filmmaker profiles, uses sexually suggestive imagery or any other unfair, misleading or deceptive Content intended to draw traffic to the profile.

The following is a partial list of the kind of activity that is illegal or prohibited on the MySpace Website and through your use of the MySpace Services. MySpace.com reserves the right to investigate and take appropriate legal action against anyone who, in MySpace.com's sole discretion, violates this provision, including without limitation, reporting you to law enforcement authorities. Prohibited activity includes, but is not limited to:

1. criminal or tortious activity, including child pornography, fraud, trafficking in obscene material, drug dealing, gambling, harassment, stalking, spamming, spimming, sending of viruses or other harmful files, copyright infringement, patent infringement, or theft of trade secrets;
2. advertising to, or solicitation of, any Member to buy or sell any products or services through the MySpace Services. You may not transmit any chain letters or junk email to other Members. It is also a violation of these rules to use any information obtained from the MySpace Services in order to contact, advertise to, solicit, or sell to any Member without their prior explicit consent. In order to protect our Members from such advertising or solicitation, MySpace.com reserves the right to restrict the number of emails which a Member may send to other Members in any 24-hour period to a number which MySpace.com deems appropriate in its sole discretion. If you breach this Agreement and send unsolicited bulk email, instant messages or other unsolicited communications of any kind through the MySpace Services, you acknowledge that you will have caused substantial harm to MySpace.com, but that the amount of such harm would be extremely difficult to ascertain. As a reasonable estimation of such harm, you agree to pay MySpace.com \$50 for each such unsolicited email or other unsolicited communication you send through the MySpace Services;
3. covering or obscuring the banner advertisements on your personal profile page, or any MySpace.com page via HTML/CSS or any other means;
4. any automated use of the system, such as using scripts to add friends or

- send comments or messages;
5. interfering with, disrupting, or creating an undue burden on the MySpace Services or the networks or services connected to the MySpace Services;
  6. attempting to impersonate another Member or person;
  7. for band profiles, copying the code for your MySpace Player and embedding it into other profiles or asking other Members to embed it into their profiles;
  8. using the account, username, or password of another Member at any time or disclosing your password to any third party or permitting any third party to access your account;
  9. selling or otherwise transferring your profile;
  10. using any information obtained from the MySpace Services in order to harass, abuse, or harm another person;
  11. displaying an advertisement on your profile, or accepting payment or anything of value from a third person in exchange for your performing any commercial activity on or through the MySpace Services on behalf of that person, such as placing commercial content on your profile, posting blogs or bulletins with a commercial purpose, selecting a profile with a commercial purpose as one of your "Top 8" friends, or sending private messages with a commercial purpose; or
  12. using the MySpace Services in a manner inconsistent with any and all applicable laws and regulations.
9. **Copyright Policy.** You may not post, modify, distribute, or reproduce in any way any copyrighted material, trademarks, or other proprietary information belonging to others without obtaining the prior written consent of the owner of such proprietary rights. It is the policy of MySpace.com to terminate Membership privileges of any Member who repeatedly infringes the copyright rights of others upon receipt of prompt notification to MySpace.com by the copyright owner or the copyright owner's legal agent. Without limiting the foregoing, if you believe that your work has been copied and posted on the MySpace Services in a way that constitutes copyright infringement, please provide our Copyright Agent with the following information: (i) an electronic or physical signature of the person authorized to act on behalf of the owner of the copyright interest; (ii) a description of the copyrighted work that you claim has been infringed; (iii) a description of where the material that you claim is infringing is located on the MySpace Services; (iv) your address, telephone number, and email address; (v) a written statement by you that you have a good faith belief that the disputed use is not authorized by the copyright owner, its agent, or the law; (vi) a statement by you, made under penalty of perjury, that the above information in your notice is accurate and that you are the copyright owner or authorized to act on the copyright owner's behalf. MySpace.com's Copyright Agent for notice of claims of copyright infringement can be reached as follows: Copyright Agent, MySpace.com, Inc. 6060 Center Drive, Suite 300; Los Angeles, CA 90045; telephone: (310) 917-4923; facsimile: (310) 394-4180 Attn: Copyright Agent; and email: [copyrightagent@myspace.com](mailto:copyrightagent@myspace.com).
10. **Member Disputes.** You are solely responsible for your interactions with other MySpace.com Members. MySpace.com reserves the right, but has no obligation,

to monitor disputes between you and other Members.

11. **Privacy.** Use of the MySpace Services is also governed by our Privacy Policy, which is incorporated into this Agreement by this reference.
12. **Disclaimers.** MySpace.com is not responsible for any incorrect or inaccurate Content posted on the MySpace Website or in connection with the MySpace Services, whether caused by Users of the MySpace Services or by any of the equipment or programming associated with or utilized in the MySpace Services. Profiles created and posted by Members on the MySpace Website may contain links to other websites. MySpace.com is not responsible for the Content, accuracy or opinions expressed on such websites, and such websites are in no way investigated, monitored or checked for accuracy or completeness by MySpace.com. Inclusion of any linked website on the MySpace Services does not imply approval or endorsement of the linked website by MySpace.com. When you access these third-party sites, you do so at your own risk. MySpace.com takes no responsibility for third party advertisements which are posted on this MySpace Website or through the MySpace Services, nor does it take any responsibility for the goods or services provided by its advertisers. MySpace.com is not responsible for the conduct, whether online or offline, of any User of the MySpace Services. MySpace.com assumes no responsibility for any error, omission, interruption, deletion, defect, delay in operation or transmission, communications line failure, theft or destruction or unauthorized access to, or alteration of, any User or Member communication. MySpace.com is not responsible for any problems or technical malfunction of any telephone network or lines, computer online systems, servers or providers, computer equipment, software, failure of any email or players due to technical problems or traffic congestion on the Internet or on any of the MySpace Services or combination thereof, including any injury or damage to Users or to any person's computer related to or resulting from participation or downloading materials in connection with the MySpace Services. Under no circumstances shall MySpace.com be responsible for any loss or damage, including personal injury or death, resulting from use of the MySpace Services, attendance at a MySpace.com event, from any Content posted on or through the MySpace Services, or from the conduct of any Users of the MySpace Services, whether online or offline. The MySpace Services are provided "AS-IS" and as available and MySpace.com expressly disclaims any warranty of fitness for a particular purpose or non-infringement. MySpace.com cannot guarantee and does not promise any specific results from use of the MySpace Services.
13. **Limitation on Liability.** IN NO EVENT SHALL MYSPACE.COM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, SPECIAL OR PUNITIVE DAMAGES, INCLUDING LOST PROFIT DAMAGES ARISING FROM YOUR USE OF THE SERVICES, EVEN IF MYSPACE.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED HEREIN, MYSPACE.COM'S LIABILITY TO YOU FOR ANY CAUSE WHATSOEVER AND REGARDLESS OF THE FORM OF THE ACTION, WILL AT ALL TIMES BE LIMITED TO THE AMOUNT PAID, IF ANY, BY YOU TO MYSPACE.COM FOR THE MYSPACE SERVICES DURING THE TERM OF MEMBERSHIP.
14. **U.S. Export Controls.** Software available in connection with the MySpace Services (the "Software") is further subject to United States export controls. No Software may be downloaded from the MySpace Services or otherwise exported or re-exported in violation of U.S. export laws. Downloading or using the Software

is at your sole risk.

15. **Disputes.** If there is any dispute about or involving the MySpace Services, you agree that the dispute shall be governed by the laws of the State of California, USA, without regard to conflict of law provisions and you agree to exclusive personal jurisdiction and venue in the state and federal courts of the United States located in the State of California, City of Los Angeles. Either MySpace.com or you may demand that any dispute between MySpace.com and you about or involving the MySpace Services must be settled by arbitration utilizing the dispute resolution procedures of the American Arbitration Association (AAA) in Los Angeles, California, USA, provided that the foregoing shall not prevent MySpace.com from seeking injunctive relief in a court of competent jurisdiction.
16. **Indemnity.** You agree to indemnify and hold MySpace.com, its subsidiaries, and affiliates, and their respective officers, agents, partners and employees, harmless from any loss, liability, claim, or demand, including reasonable attorneys' fees, made by any third party due to or arising out of your use of the MySpace Services in violation of this Agreement and/or arising from a breach of this Agreement and/or any breach of your representations and warranties set forth above and/or if any Content that you post on the MySpace Website or through the MySpace Services causes MySpace.com to be liable to another.
17. **Other.** This Agreement is accepted upon your use of the MySpace Website or any of the MySpace Services and is further affirmed by you becoming a Member. This Agreement constitutes the entire agreement between you and MySpace.com regarding the use of the MySpace Services. The failure of MySpace.com to exercise or enforce any right or provision of this Agreement shall not operate as a waiver of such right or provision. The section titles in this Agreement are for convenience only and have no legal or contractual effect. MySpace.com is a trademark of MySpace, Inc. This Agreement operates to the fullest extent permissible by law. If any provision of this Agreement is unlawful, void or unenforceable, that provision is deemed severable from this Agreement and does not affect the validity and enforceability of any remaining provisions.

Please contact us at: [Contact MySpace](#) with any questions regarding this Agreement.

I HAVE READ THIS AGREEMENT AND AGREE TO ALL OF THE PROVISIONS CONTAINED ABOVE.

MR. WHITFIELD. Thank you, very much, and that was quite effective. I appreciate your sharing that with us.

Mr. Hiler, you are recognized for 5 minutes.

MR. HILER. Chairman Whitfield, Ranking Member Stupak and members of the subcommittee, my name is John Hiler and I am the CEO and cofounder of Xanga.com. I ask that a copy of my full statement appear in the record.

Thank you for inviting me to testify at today's hearing. I would like to take a couple of minutes to talk about Xanga. First and foremost, Xanga is a place to write. Xanga was founded in 1999 as a way for authors to publish their ideas on the Internet. Xanga's predominant use today continues to be publishing in the form of Web logs. Web logs, or blogging, are a form of online publishing characterized by relatively frequent posts arranged in reverse chronological order.

In April of this year, Xanga added limited social networking features to its site but, as used by our members, our site remains primarily a place to write. As I like to put it, the vibe on Xanga is much more like a cafe than a nightclub. To preserve its literary focus, Xanga has been careful not to enable certain features that are typical of more socially or dating-oriented websites. Xanga does not allow users to search for each other by specific demographic characteristics. For example, you cannot search Xanga profiles for a 24-year-old woman from Kentucky who may be single. Xanga also decidedly does not provide features such as instant messaging, chat, private message between members, or real-time gold tones. We feel strongly that these features need strong safety filters in place before we would feel comfortable launching them, especially since these form of communications occur privately rather than in public.

Our members use the site in many ways including as a creative outlet, as a way to explore personal identity and spirituality and as a source of support for difficult issues. For example, Xanga has over 8,500 groups focused on poetry, almost 40,000 groups dedicated to Christianity and over 2,000 groups that are dedicated to parenting issues including support for first-time parents, stay-at-home parents, and single parents.

As an industry leader, Xanga is committed to being at the forefront of Web log communities when it comes to looking out for the safety of all of our users. There is no single silver bullet but we are committed to trying any solution that is feasible. What makes Xanga unique is its comprehensive approach that empowers members, parents, and Xanga itself all to take charge of online safety.

I would like to highlight two technologies that Xanga has developed to empower its members to help police its site. They are a rating system and a flagging system. While both systems are still new and being refined, these technologies have received strong initial reviews from both our members and from industry experts.

Our first safety initiative is a rating system. To address the issue of clean content, we have created a rating system, a picture of which you can see attached to the back of our written testimony. As you can see, it is a five-part rating system modeled after the system used to rate motion pictures. This rating system launched on May 26 of this year and we use the ratings to limit access to age-inappropriate content including requiring a credit card before members can view sites rated as containing adult material.

Our second important safety program is a flagging system that Xanga has developed to allow users to easily report sites that violate Xanga's terms of use. This system launched on May 1 of this year has been extremely effective in rapidly identifying inappropriate content. Now if a Xanga member sees a page with inappropriate content, he or she can view a list of potential flags with just a single click. Then with just one more click, that site or page can be instantly reported to our flagging database. Flagged sites are reviewed by Xanga's trained analysts and shut down as appropriate. Depending on the nature of the flag, these sites may also be reported to the proper authorities such as the National Center for Missing and Exploited Children, also known as NCMEC.

Mr. Chairman, as you pointed out yesterday, it is very important that we get sites with child porn off of the site as quickly as possible. With our flagging system, we have been able to identify, delete, and report these sites to NCMEC in as quickly as a few hours.

Xanga has also embraced best practices in data retention and preservation, an issue that I know is important to the committee. Xanga records IP addresses for every user upon registration, retains that information indefinitely for law enforcement. Our practice is to comply with all subpoenas within one to two business days if not significantly faster. Xanga is also working with the National Center's cyber tip line to identify other points at which to capture IP addresses including during photo uploads and during member sign-ins. As soon as our recommendations are finalized, we will implement them and begin retaining and preserving this additional IP information as well.

We have also recently launched several other privacy features which empower users to control and monitor access to their own sites, not only increasing their own privacy, but also making their site safer as well.

In addition, I want to reiterate what features Xanga does not support: instant message, chat, private messaging, private bulletins, and profile search. We are also working with experts so our site reflects industry best practices including WiredSafety, the National Center and Blogsafety.com, and finally, Xanga routinely works with law enforcement to help with investigations.



We at Xanga are fully committed to ensuring the safest possible environment for our members. There is no single silver bullet out there to guarantee the safety of our members but we are committed to a comprehensive approach involving technology, empowering our users and cooperating with law enforcement and industry experts.

Thank you, and I look forward to answering any questions.

[The prepared statement of John Hiler follows:]

PREPARED STATEMENT OF JOHN HILER, CHIEF EXECUTIVE OFFICER, XANGA.COM, INC.

Chairman Whitfield, Ranking Member Stupak, and members of the subcommittee, my name is John Hiler, and I am co-founder and CEO of Xanga.com. Thank you for inviting me to testify at today's hearing, and we at Xanga look forward to hearing from the other witnesses and members of the subcommittee on this important issue.

#### **WHAT IS XANGA?**

Xanga is a place to write.

Xanga was founded in 1999 as a service for authors to publish their ideas on the internet. I had recently written a book on Japanese language and wanted to build a website to publish the book. But at that time it was easier to learn Japanese than build a website where people could easily post content. Xanga was founded to address that challenge.

Today, Xanga has over 27 million registered users and has grown into an industry leader. In May 2006, Alexa Internet, a site that provides information on web traffic, rated Xanga as the 21st most popular English-language website and the 42nd most popular website in the world.

Xanga's predominant use today – a use which became predominant early in Xanga's history - is "weblogging" (also known as "blogging"). It is a form of online

publishing characterized by relatively frequent posts arranged in reverse-chronological order (the newest posts appear first). Weblogging encourages discussion in the form of “comments.” Owners of Xanga weblogs (which we call “Xanga Sites”) can allow other users to leave comments on any individual post, to get feedback on ideas and help push ideas in new directions.

Starting in 2002, with the emergence of innovative sites like Friendster, a new form of online interaction exploded onto the scene: “social networking.” The predominant use of a social networking website is to publish an online profile – including demographic information, interests, and the like – and to connect to other profiles to create online networks.

In 2005, Xanga’s members began asking for a way to better connect with friends and family online. In response to these requests, in April 2006, the company added limited social networking features to its site. But as used by our members, Xanga remains primarily a place to write. Xanga remains more of a publishing site than a social network. As I like to say, the “vibe” of Xanga is much more like a café than a nightclub.

To preserve its literary focus, Xanga has been careful *not* to enable certain features that are typical of more social-focused or dating-oriented websites. Xanga does *not* allow users to search for each other by specific demographic characteristics (e.g. you cannot search Xanga Profiles for 24 year-old, women from Kentucky who are single). Xanga also decidedly does not provide features such as instant messaging, chat and private messaging between members. Xanga feels strongly that these features need strong safety filters in place before we would feel comfortable launching them, especially since these forms of communication occur privately rather than in public.

The huge number of users participating in this blogging phenomenon, and the sheer volume of content generated by these users, create unique challenges in addressing today's concerns over online safety. But Xanga is committed to a comprehensive approach to online safety, and we think we have promising technology solutions that address the challenges posed by the sheer volume of users and content. We'll discuss these solutions later in this testimony.

#### **EXAMPLES OF XANGA USE**

Xanga members use the site in many ways - including as a creative outlet, as a way to explore personal identity and spirituality, and as a source of support for difficult issues:

- **CREATIVE OUTLET** – Xanga started as a literary site and today has over 8,500 groups focused on poetry, over 7,000 groups focused on writing, and tens of thousands of additional groups where users share ideas on architecture, art, dancing, drama, photography and the like;
- **PERSONAL IDENTITY AND SPIRITUALITY** – the spirituality and religious community embraced Xanga almost from its beginning, as a way to share and discuss the faith. For example, today the site has almost 40,000 groups dedicated to Christianity. The most popular such group, with over 8,000 members, encourages open discussion from all denominations. Xanga has another 22,000 groups dedicated to other religions and spirituality;
- **SUPPORT GROUPS** – Xanga members have created tens of thousands of support groups covering a huge range of family issues. Xanga has over 2,000 groups that are dedicated to parenting issues, including support for first-time parents, stay-at-

home parents, single parents and even teen parents. One popular group, with almost 600 members, is described by its founder as, “The Family in Crisis - Marriage, Divorce, Separation, Death, Teenage pregnancy, abortion, missing children, housing problems, financial problems, runaway children, child abuse, parent abuse, aging parents, alcoholism, drug abuse. The family today is facing many issues that are destroying happy families. How can we deal with all these issues ? What works ? What doesn't ? Sharing our stories and remedies with each other is a good start.”

That last description beautifully summarizes the core value of Xanga to its community: “Sharing our stories and remedies with each other is a good start.” Xanga brings together individuals from all over the world so that they can share stories, learn from each other, and ideally learn a bit more about themselves in the process.

#### **BLOGS AND SOCIAL NETWORKS IN AN HISTORICAL CONTEXT**

A recurrent theme in the history of media has been the need to protect youth from inappropriate content.

Blogs and social networks have encountered this same issue as they’ve exploded in popularity. Much like comic books, movies, and video games before it, blogs and social networks draw much of their popularity from youth – who feel that the new medium speaks to them, and belongs uniquely to their generation.

Along with this explosive growth comes an inevitable backlash, as parents and their elected officials express legitimate concerns about the potentially dangerous and corruptive effects of the new medium. This pattern has emerged in virtually every past media sector:

- **MOVIES** - In 1933, religious groups warned against the "massacre of innocence of youth" and urged a campaign for "the purification of the cinema."
- **COMIC BOOKS** - In 1954, a Senate Subcommittee on Juvenile Delinquency explored connections between juvenile delinquency and the comic books industry.
- **VIDEO GAMES** - In 1993, a Senate Judiciary and Government Affairs Committee hearing was held to discuss video game violence.

Each of these industries - movies, comic books, and video games - eventually ended up embracing the same solution to protect youth: a ratings system that offers age-restricted access.

Drawing on the lessons from the history of earlier media sectors, Xanga has developed its own ratings system (see further description below). In doing so, Xanga hopes to balance the free speech rights of its users, with the need to protect youth from age-inappropriate content.

#### **XANGA AND ITS ONLINE COMMUNITY**

Our members very much want to be in an online community that is safe. Through emails and comments on our Xanga Sites, they tell us that they are pleased with our focus on safety issues. And they tell us that they want to *participate* in keeping the Xanga community as safe as possible.

In response to our community's requests, we've embraced a safety model that centers on *empowering our users to help us police and protect the community*. It's the online equivalent of a vast Neighborhood Watch program – and our users are active participants.

Our safety features, such as our ratings and flagging systems, have been well received by the community we serve because these features allow them to take part in patrolling or policing their community.

### **XANGA.COM: AN INDUSTRY LEADER COMMITTED TO SAFETY**

As an industry leader, Xanga is committed to being at the forefront of weblog communities when it comes to looking out for the safety of all its users. There is no one single silver bullet, but Xanga is committed to trying any solution that is feasible. What makes Xanga unique is its comprehensive, three-part approach that empowers members, parents and Xanga all to take charge of online safety.

#### **Part #1: Advanced Technologies on Xanga.com**

Xanga has long employed advanced technologies on its site to empower users to help police their online community and protect their privacy. Xanga is constantly working to update the existing features and develop new ones to ensure it remains an industry leader.

I would like to highlight two technologies that Xanga has developed to empower its members to help police the site, in collaboration with Xanga's abuse team: a ratings system and a flagging system. While both systems are still new and being refined, these technologies have received strong initial reviews from our members and industry experts.

I also want to touch on the lengths Xanga goes through to protect its data for potential cooperation with law enforcement entities.

#### **RATING SYSTEM**

Our first safety initiative is a rating system. To address the issue of clean content, Xanga has created a rating system that, among other things, limits access to age-

inappropriate material. A description of how the ratings system works (and looks) can be found in the attached materials.

This ratings system launched on May 26th, allowing members to self-rate their own content. Xanga uses the ratings to limit access to sites that are inappropriate for minors using various measures, including requiring a credit card before members can view sites rated as containing explicit material.

In the event that members are not honest about their self-ratings, Xanga has also built in two safety measures:

First, members are empowered to rate each others' sites; the resultant ratings are then blended together to create a consensus rating for each site or page. These Community Ratings represent the community norm. Of course, not everyone can be trusted to rate sites honestly – so again, we have used an algorithm that detects whether or not a user can be trusted to rate sites reliably. If they can, then their ratings votes are weighted more heavily; if they can't, then they are weighted less heavily.

We have also built in an additional safeguard, where Xanga administrators have the ability to rate sites and override both the Self Rating and the Community Rating.

To assist in this Ratings initiative, Xanga has retained Dr. Arthur Pober as a consultant. Dr. Pober is the former head of the Children's Advertising Review Unit (CARU), founding president of the ESRB (the video game ratings association) and a leading published expert on ratings systems. Dr. Pober is advising Xanga on the design and implementation of its ratings system.

### **FLAGGING SYSTEM**

Our second important safety program is a flagging system that Xanga has developed to allow users to easily report sites that violate Xanga's terms of use. The flagging system launched on May 1, 2006, and has been very effective in rapidly identifying inappropriate content.

In the past, Xanga found that we were not receiving a high volume of reports of inappropriate or illegal content. An investigation revealed the root cause of the problem: the process of reporting inappropriate content on most sites was simply too difficult.

This was a common issue across the blogging and social networking industry.

As a result, Xanga designed and deployed a "one click" flagging system. Now if a Xanga member sees a page with inappropriate content, he or she can view a list of potential flags with just a single click. Then with one more click, that site or page is instantly reported to the Xanga flagging database.

Flagged sites are reviewed by Xanga's trained analysts and shut down as appropriate. Depending on the nature of the flag, these sites may also be reported to the proper authorities, such as the National Center for Missing & Exploited Children (NCMEC). Xanga is a participating member of the NCMEC's CyberTipline, which serves as a clearing house for reports of child pornography. And our new flagging system has significantly enhanced Xanga's ability to help NCMEC combat this issue.

### **FLAGGING SYSTEM CASE STUDY: CHILD PORN**

I recently had the opportunity to attend the Social Networking Dialogue hosted by the National Center for Missing & Exploited Children's (NCMEC). Several of the panels highlighted a new insidious form of child porn: the self-exploitation of youth. With the



advent of web-based publishing tools, youth are increasingly taking photos of themselves without clothes on, and then posting these photos online.

We believe this is one of the more concerning developments in user-generated content, and we've taken every step we can to address this threat.

In cases of self-exploitation, it is absolutely crucial to take these photos down as quick as possible – before they fall into the hands of those who might distribute them further. This is where Xanga's new flagging system really shines. Xanga's 27 million members are each empowered to flag any sites that appear to contain child porn. Then the flagged sites are reviewed by Xanga's analysts, and any confirmed reports of child porn are shut down and reported to NCMEC's CyberTipline, as required by law.

Any flagging system will receive a fair number of false reports, and Xanga's system is no different. We have addressed this by incorporating an algorithm we call, "The Boy Who Cried Wolf." If a user flags a site and there is no "wolf" (in this case, child porn), then in the future, we know that that user isn't very credible. Conversely, if a user flags a site and there is child porn, then in the future, we know that the flagger is especially credible. The result is that over time, Xanga's flagging system has gotten smarter and smarter as it has learned which users are reliable.

As the flagging system has learned who to trust, we have seen the emergence of reliable child protection advocates who surf the Xanga site looking for inappropriate material. These advocates are finding and flagging this material very quickly; our analysts immediately review these flags and delete/report the material right away.

**DATA RETENTION AND PRESERVATION**

Xanga has embraced best practices in data retention and preservation.

Xanga records IP addresses for every user upon registration and retains that information indefinitely for law enforcement.

As required by law, Xanga will cooperate with law enforcement by sharing IP information upon receipt of a subpoena. If a clear crime has been committed – such as uploading child porn – Xanga will proactively share IP information with the appropriate authorities (in this case, with NCMEC’s CyberTipline).

Xanga’s practice is to comply with all subpoenas within 1-2 business days, if not significantly faster.

In addition to retaining and preserving IP addresses upon member registration, Xanga is working with NCMEC’s CyberTipline to identify other points at which to capture IP addresses (e.g. during photo uploads, during most recent member sign-in, etc.). As soon as NCMEC’s recommendations are finalized, we will implement them and begin retaining and preserving this additional IP information as well.

**PRIVACY**

Xanga has also recently launched several other privacy features, which empower users to control and monitor access to their own sites, not only increasing their privacy, but making them safer as well:

**Xanga Footprints**

With Xanga Footprints, any participating Xanga member can see the usernames of signed-in visitors to their site. If visitors are not signed in, then the country or state is shown instead.

Xanga supports an “opt out” for this feature, much as the phone companies do for Caller ID. Xanga is also working on a Footprint Lock, which allows members to allow only visitors who have not opted out of Footprints.

#### **Xanga Lock:**

With Xanga Lock, only other Xanga members can get access to a given site. This not only hides the site from outsiders, it also prevents the site from being indexed by search engines. Xanga Lock combines with the Footprints feature to provide a powerful method for controlling and monitoring access to a given site.

#### **PROTECTED POSTING**

This feature allows users to restrict access of each post to a list of specified friends.

#### **USER BLOCKING**

Xanga also supports user blocking, which allows users to block certain people from commenting or subscribing to their sites.

In addition to all of these safety and privacy features, it is important to reiterate what features Xanga does *not* support: instant message, chat, private messaging, private bulletins, and profile search (i.e. the ability to search profiles for specific demographic characteristics).

#### **Part #2: Screening Out Underage Users**

Xanga has adopted best practice recommendations for screening out underage users during the registration process. These recommendations, made by the Children’s Advertising Review Unit of the Better Business Bureau, include using neutral age-

screening and session cookies. These tools help prevent children under the age of 13 from joining the site, let alone entering private information.

Finally, in the event that a user lies about his or her age in order to evade Xanga's safety measures, Xanga has also recently hired additional staff whose sole responsibility is to respond to reports and inquiries from parents. Xanga's current policy is to act upon all account deletion requests from parents within two business days, and many requests are processed faster than that.

### **Part #3: Cooperation With Industry Experts and Law Enforcement**

Xanga is actively working with experts so its site reflects industry best practices.

#### **WIREDSAFETY.ORG**

Xanga works with WiredSafety.org to incorporate industry best practices on its site. Based on input from WiredSafety.org founder Parry Aftab, Xanga has developed a separate section on its site dedicated to online safety, *safety.xanga.com*, which includes safety tips to empower teens, parents and law enforcement to take steps to stay safe in their online community. This safety section is linked to from every page on every Xanga site.

Xanga has also submitted its site for general safety review by WiredSafety.org and is currently participating in an industry effort to help define best practices for social networking sites.

On June 21, Xanga participated in WiredSafety.org's Social Networking Summit. This event brought together law enforcement, industry experts, and several of WiredSafety's "Teenangels" to discuss new and better ways to keep youth safe online.

Xanga's President, Marc Ginsburg, and I both participated on panels exploring the facts and the future of blogging and social networking. It was particularly interesting to hear from the young people who offered their thoughts on how they use blogging and social networking sites and how we can work together to keep them safe.

#### **THE NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN**

On June 22, Xanga participated in the National Center for Missing & Exploited Children's (NCMEC) "Social Networking Dialogue" where representatives of social networking sites met with public officials and law enforcement to discuss how best to address industry issues such as youth safety. I participated in a panel discussion in which I described Xanga's Rating System and other safety initiatives.

The NCMEC dialogue was a good opportunity for many experts and industry leaders to come together to share ideas about how we can work to make our medium as safe as possible for all our users, especially children. We believe that every idea or recommendation deserves a place at the table.

#### **BLOGSAFETY.COM**

Xanga has become a founding supporter of BlogSafety.com, an online safety forum for parents, teens, educators, and advocates. BlogSafety.com is a project of Tech Parenting Group, a nonprofit organization based in Palo Alto, California, and Salt Lake City, Utah. The forum is co-directed by Larry Magid of SafeKids.com and Anne Collier of NetFamilyNews.org.

#### **LAW ENFORCEMENT**

Xanga routinely works with law enforcement to help with investigations. To ensure that we don't violate users' privacy, we do ask that police investigators send us a

subpoena before we pass along any user information. But Xanga has made it a point to respond to any such subpoena within 1-2 business days (and typically within hours).






To make it easier for law enforcement to get through to Xanga in the course of any investigation, and particularly in case of emergencies, Xanga has recently added a link on the bottom of every Xanga Site for, "Law Enforcement." That link points to a special page on Xanga's new safety site ([safety.xanga.com](http://safety.xanga.com)) with resources specifically for law enforcement, including a prominent link to contact Xanga.

### **CONCLUSION**

Xanga is fully committed to ensuring the safest possible environment for its members. However, there is no single silver bullet out there to guarantee the safety of our members or those of other social networks. Instead, a comprehensive approach is needed involving technology, cooperation with industry experts and law enforcement and human oversight.

For its part, Xanga is aggressively working to develop and implement advanced technologies on its site to help protect its members. We are reaching out to industry experts to learn more about how we can implement best practices. And we are reaching out to the media, families and safety experts to explain the safety features of Xanga.

Thank you and I look forward to answering any questions.

MPAA		XANGA	
<b>G</b> <b>GENERAL AUDIENCES</b> All Ages Admitted		<b>a</b> <b>all ages allowed</b>	
<b>PG</b> <b>PARENTAL GUIDANCE SUGGESTED</b> SOME MATERIAL MAY NOT BE SUITABLE FOR CHILDREN		<b>b</b> <b>basic guidance</b> some material may not be suitable for young children	
<b>PG-13</b> <b>PARENTS STRONGLY CAUTIONED</b> Some Material May Be Inappropriate for Children Under 13		<b>c</b> <b>caution</b> some material may be inappropriate for children	
<b>R</b> <b>RESTRICTED</b> UNDER 17 REQUIRES ACCOMPANYING PARENT OR ADULT GUARDIAN		<b>d</b> <b>discretion required</b> parent or guardian approval required for minors	
<b>NC-17</b> NO ONE 17 AND UNDER ADMITTED		<b>ex</b> <b>explicit content</b> adults only, no one under 18 allowed	

MR. WHITFIELD. Thank you very much, Mr. Hiler, and Mr. Angus, I want to thank you again for bringing that public service announcement that you all are utilizing, and at this time, on my time, I do want to show the public service announcement that is being used in Great Britain that was prepared by the Virtual Global Taskforce. This public service announcement is being shown in movie theaters around Great Britain.

MR. WHITFIELD. The sound works very well. We will try one more minute. If it doesn't work, we will move on.

[Video].

MR. WHITFIELD. I would ask each one of you that report abuse, do you have a technique like that on your space, Mr. Kelly?

MR. KELLY. Yes. I mean, you will have a report, this photo report this message report. I mean, there are reporting tools built in throughout the site.

MR. WHITFIELD. And easily available?

MR. KELLY. Easily available.

MR. WHITFIELD. Mr. Angus?

MR. ANGUS. Likewise on each page within MySpace, there is a link to report abuses of content. There are also links on each photo that is hosted by MySpace to report photos themselves, and then if a photo is reported, you are then permitted as a user to respond and forward that information onto the National Center's cyber tip line.

MR. WHITFIELD. Cyber tip line. Okay.

MR. HILER. Yes. At Xanga we absolutely have a link on every single page that links to our flagging technology I mentioned before. We have identified around 10 separate, we call them crimes, that users can report. One of these is for child porn and we built some additional technology that enables us to identify which pages are being flagged most frequently for child porn and we prioritize our resources on those reports so we can send them right to the National Center.

MR. WHITFIELD. So the flagging occurs first and then to the cyber tip line?

MR. HILER. There is a middle layer where our trained analysts take a look at the images.

MR. WHITFIELD. In the testimony today and throughout these hearings, we have heard a lot about young people who are not truthful about their age, and I would like to ask all of you if you have any flagging or filtering device to match up what a person in their profile says their age is and information that might reveal what their actual age is?

MR. KELLY. So again, we take a somewhat different approach because of our segmented networks so users have to verify where we can with dot edu or dot org email addresses into high school communities, and if not with an invitation method from validated users into that high school community. So there is a proxy for age. They are also required to put their birth date, and in proper compliance, we assure that that is a birth date calculation. We don't ask are you over 13 or something like that. We don't allow anyone to register for a high school class that wouldn't make them 13. So we have a variety of proxy methods for age but, obviously are interested in finding more certain verification.

MR. WHITFIELD. Right. Mr. Angus?

MR. ANGUS. MySpace only permits users 14 years and older to join the site, and it is a similar process where the user is required to enter in a birth date and then the calculation is made. If they enter in a birth date



that results in that individual being too young, a session cookie is placed on the computer and they are not permitted to back button and then just fix the date. In addition, we do have a proprietary search algorithm that constantly scans the site looking for phrases that users use to identify themselves as being underage. Again, this is a site where users are there to talk about themselves and portray themselves to their community of friends and so frequently we see them using either in code or in actual language saying I am really 13 and then we have a team of security experts go through each reported instance and to determine whether it is an individual saying my daughter is 13, my dog is 13 or I am 13, and every user that we identify as being under the age of 14 is deleted from the site and banned.

MR. WHITFIELD. So you have an ongoing screening process that is looking at different--

MR. ANGUS. That is correct, and we constantly update the search phrases as the users change their terminology. One of the popular ones right now is cake date instead of birth date.

MR. WHITFIELD. And they are automatically banned from the site--

MR. ANGUS. Yes.

MR. WHITFIELD. --if they are determined to be--

MR. ANGUS. That is correct.

MR. WHITFIELD. Have you had any legal ramifications with trying to do that or doing that?

MR. ANGUS. No, we have not.

MR. WHITFIELD. Mr. Hiler?

MR. HILER. In addition to the standard ways that we all screen underage users from joining our site, we have two separate failsafes. The first is a parental deletion request form. We have created a policy and procedure through which parents can send us a signed consent form asking that we delete the account. We generate an archive and we send it to them. So that is one. The second is that as part of our theme of empowering the user, we have created a flag that says "proof of underage user" and that way users can flag sites that they believe have people who are underage. We can take a look at the sites that have been flagged by the community and evaluate them, and what we find often is that it is older brothers and sisters who are on the site who want to police their younger brothers and sisters from joining us and so it has been nice to see that pattern of self-policing emerge.

MR. WHITFIELD. So if a parent contacts any of you and demands that you take down a child's profile, will all of you do that?

MR. KELLY. So we--

MR. WHITFIELD. Your situation is a little different.

MR. KELLY. Our situation is a little bit different. We have actually a problem that we have identified legally under the Electronic Communications Privacy Act about giving a parent access to an account. So we certainly encourage parents to talk with their student user and if they can get their password and sign into their account, well, obviously we have an easy deactivation process. So we try to work with the parents in those instances. But there is no underage exception for ECPA and so we have been concerned about legal liability from that standpoint if we give parents access to the account.

MR. WHITFIELD. But to get on your site, I have to have a university address--

MR. KELLY. Well, if you have a validated high school user either through--if the high school issues its own address--that is our preferred method. That is our favorite way to assure that the user is in fact associated with that school. Otherwise we use an invitation method which we started by having confirmed college users invite people at their old high schools and then have this validation method over time. So there are high school students on the site where we will get requests from parents to take it down and we try to facilitate that analysis without exposing ourselves to legal liability under ECPA.

MR. WHITFIELD. And Mr. Angus, what about MySpace?

MR. ANGUS. We do honor parents' requests to take down profiles of users under the age of 14. The issue that we have is that in some cases this is a form of cyber bullying and we will find that some teens may purport to be parents of that user and attempt to have that user's account deleted, so we do work with the parents to verify that they are actually the parent of that individual. In addition to just removing underage profiles, if a parent of a 14-, 15-, 16- or 17-year-old wants their child's profile deleted, we will also do that upon verification. Of course, we always encourage the parents to communicate directly with their kids, because as the detective indicated, once the teens are banned, frequently they will just go underground and that makes them more reticent to discuss issues that can arise.

If I could just address your previous comment about automatically searching, we also have a number of users who value the community and also get reports from our user base about underage profiles.

MR. WHITFIELD. My time is expired but one thing that I would like for you to do, Mr. Angus, is that we have a copy of a letter from the Attorney General of Ohio dated March 24, 2006, to Mr. Chris DeWolf, who I guess was the CEO of MySpace.com. I am not sure when Fox purchased that but I don't know if you are even familiar with this letter but in his letter he suggests certain ways to address some of these issues,

and I would like to give you a copy of it and maybe you can just respond to the committee in writing.

MR. ANGUS. Certainly. I would be happy to do that.

MR. WHITFIELD. And at this time I would like to recognize Mr. Stupak.

MR. STUPAK. Thank you. The Chairman was asking about reporting of abuses. Let us go down the line and answer these questions. Mr. Kelly, if I am going to report abuse, who would I report it to if I am on your network?

MR. KELLY. So on our site, it would go to our customer service staff.

MR. STUPAK. And then what happens to it?

MR. KELLY. So it is reviewed by--we have a customer service staff of 20 who are all recent graduates and very experienced in Facebook. I like to say we have the most overeducated customer service staff in America. They are all recent graduates of great universities and they assess whether or not there is a complaint about the violation in terms of service or an underage user or whatever may come, they assess it quickly. If it is a valid complaint, they process it in accordance, usually within 24 hours.

MR. STUPAK. If it is a valid complaint, process it how?

MR. KELLY. So if it is an underage user, we boot the user. If it is an inappropriate photo, a violation of the terms of service, we remove the photo and the user gets a warning the first time. They get a second sterner warning and a suspension the second time, and the third time their account is permanently barred. Unlike most other sites--

MR. STUPAK. Are you reporting them to NCMEC?

MR. KELLY. So if it is a child porn case, of course we report it to NCMEC and we are registered with NCMEC as a reporting agency.

MR. STUPAK. Has that ever happened?

MR. KELLY. We have not ever had an instance.

MR. STUPAK. Out of 29 million, or what do you have? How many?

MR. KELLY. Actually at this point we have about 350 million photos on our site, and because they are all students, they are posting their own pictures.

MR. STUPAK. And none of them are ever--

MR. KELLY. What?

MR. STUPAK. None of them were ever pornographic?

MR. KELLY. So some of them are inappropriate but they are not pornographic.

MR. STUPAK. Who makes that determination?

MR. KELLY. We make that determination.

MR. STUPAK. I know these are experts in computing, not necessarily in pornography.

MR. KELLY. Well, they are actually able to make the determination if there is any exploitation shown anywhere in the site and we talked with NCMEC extensively about this, they don't want a lot of false reports.

MR. STUPAK. I am not--

MR. KELLY. They are concerned about the assessment. The way that we segment our communities and the way that people share photos, we are not a haven in any way for people who would share child pornography. It is very difficult for predators to get on our site--

MR. STUPAK. Let me go on down the line now. I have only a couple minutes here. I don't want to use up all my time. Mr. Angus, how about you? Where do you guys report your uses to and where does it go and--

MR. ANGUS. Again, the link on every page, there is a drop-down menu that allows a user to categorize, and for our security time it prioritizes the abuse reports that we get. Those reports go to our safety and security team which is led by our chief security officer.

MR. STUPAK. How many people do you have on that team?

MR. ANGUS. I don't know the answer to that question. I can get back to this committee.

MR. STUPAK. Have you reported any to NCMEC, the National Center for Missing--

MR. ANGUS. Yes. Any image that involves potential child exploitation is immediately forwarded to the National Center.

MR. STUPAK. Have you?

MR. ANGUS. To be honest, as Facebook, our site is not really a haven for children.

MR. STUPAK. I am not asking that.

MR. ANGUS. But I can tell you, of the 60 million images that are uploaded to our site every month, we average approximately a dozen reports to the National Center.

MR. STUPAK. Twelve out of 60 million?

MR. ANGUS. Twelve out of 60 million, correct.

MR. STUPAK. And Mr. Hiler?

MR. HILER. Yes. Reports come in to our site in several ways. We talked about flags, we talked about ratings and of course, we get emails as well. To answer your specific question around NCMEC, we prioritize the most urgent flags. Those are child porn and death threats, threat of physical harm, to respond to. And well, we have a different story to tell. Ever since we launched our flagging system where our members can help police the site, we have gotten a lot of reports. We have gotten over--

MR. STUPAK. What happens to the reports?

MR. HILER. We have over 200 reported incidents. They are all examples of a new trend--

MR. STUPAK. Yeah, but where do they go?

MR. HILER. Of course--

MR. STUPAK. I don't want long explanations. I have only got 10 minutes.

MR. HILER. They are shut down and they are reported to the National Center. We are a participant in--

MR. STUPAK. Have you sent them to the National Center then?

MR. HILER. Yes. I was there just last week.

MR. STUPAK. I could be wrong on this but let me ask this question. Mr. Angus, did you indicate that credit companies will not allow you to use their database to verify ages of people? Was that part of your testimony?

MR. ANGUS. That was not part of my testimony. It is my understanding though, Congressman, that they do not permit us to use their facilities to verify age, that they require charges.

MR. STUPAK. Require charges. Mr. Hiler, didn't you say you used credit card companies to verify ages?

MR. HILER. We have used it to verify the ages of members over 18 to get access to the highest levels. We have been talking with our merchant account and they have expressed concerns about using it for age verification, so we are looking into alternate forms of ID verification.

MR. STUPAK. Either one of you, what could you do to verify ages? What would you do? When you testified that you don't have anyone under 13, how do you know that?

MR. KELLY. So it is because they are validated into the high school community. We have a neighborhood watch in those high school communities to report who doesn't belong, who is not actually in high school.

MR. STUPAK. Sure.

MR. KELLY. So that is--

MR. STUPAK. And you think that is 100 percent foolproof?

MR. KELLY. No, I don't think it is 100 percent foolproof. It is one of the reasons why we have the initial invitation system.

MR. STUPAK. Right.

MR. KELLY. And we have--

MR. STUPAK. High school, college and--

MR. KELLY. And then we have the segmentation of the community. That leads to better community reporting. It is not a perfect system but we feel it is better than not having any--

MR. STUPAK. Mr. Angus?

MR. ANGUS. At this point my understanding of any age verification technology is really a form of identity verification. It is extremely complex in the online world, as you can imagine, and it is something that we are working with the attorneys general on trying to find a solution for. This is especially complicated in the global setting of the Internet.

MR. STUPAK. Well, how about this idea of taking the 14- and 15-year-olds and segregating them all, putting them in their own separate site? I think that has been suggested to you guys, and you sort of resist that idea, right?

MR. ANGUS. Yes.

MR. STUPAK. Why?

MR. ANGUS. I think that as the detective indicated, once the younger users, those teens think that they are being segregated off, it is our belief that this encourages them to lie about their age, and without a viable means to verify that, they will lie about their age and that a lot of safety features that we employ specifically for those younger users will no longer be available to them. In addition, it drives them further underground, meaning that they are less comfortable reporting abuse and talking to trusted adults.

MR. STUPAK. But I wrote down here, you are the one who indicated--you stated, "No one less than 14 on MySpace," so I was wondering, how do you verify that? How can you make that statement?

MR. ANGUS. We don't permit anyone under 14 to be on the site.

MR. STUPAK. But you don't know there aren't people less than 14.

MR. ANGUS. Everyone that we know of who is under 14, we eliminate from the site. Yes.

MR. STUPAK. Let me ask you this, Mr. Angus. Some of the State attorneys general have requested that MySpace delete anyone who violates the terms of your contract or terms of service--excuse me--and permanently ban a user from MySpace for continuing posting prohibited links with pornography and other inappropriate material. But it seems like you don't automatically ban a user who has violated the terms of your service agreement, those have known to pose sexually explicit materials, according to the attorneys general. Why don't you guys do that?

MR. ANGUS. Actually we do do that. We do ban users. It depends on the level of severity.

MR. STUPAK. Do you have zero tolerance on that?

MR. ANGUS. Zero tolerance would mean that if a user were to post an image that violates the terms of our use--

MR. STUPAK. Paragraph five, isn't it? Is paragraph five terms of service?

MR. ANGUS. I don't have them in front of me but--

MR. STUPAK. But anyways, you don't have zero tolerance. Why not?

MR. ANGUS. Again, there are users who may post an image who are otherwise very good users, very good members of the community, and one oversight again as my colleague mentioned, we will send them a warning, we will delete that, and the next time they will be deleted from the site. Their profile will be taken down. Users who are posting a lot of pornography who are clearly and knowingly violating our terms of service--

MR. STUPAK. You have--

MR. ANGUS. --we will delete and we will ban from the site.

MR. STUPAK. But you report that you have 60 million images a month?

MR. ANGUS. Sixty million images a month that we--

MR. STUPAK. You don't scan those 60 million every month, do you?

MR. ANGUS. We do. Every image we review that is uploaded to our site. That is three million a day.

MR. STUPAK. And 12 reports.

MR. ANGUS. Say again.

MR. STUPAK. And 12 reports a month?

MR. ANGUS. Twelve reports to the National Center's cyber tip line. We remove approximately 1,000 images of the three million for inappropriate content.

MR. STUPAK. You remove 1,000?

MR. ANGUS. Correct.

MR. STUPAK. The other suggestion the attorneys general had was that MySpace increase the minimum user age from 14 to 16 and prohibit adult users from accessing the profiles of minors. Why do you resist that increase from 14 to 16?

MR. ANGUS. The resistance, Congressman, for increasing the age from 14 to 16 again goes to that issue of balancing. Whether you make the site too restrictive and you encourage them to lie about their age, driving them further underground and denying them the safety features that we implement for 14- and 15-year-olds.

MR. STUPAK. But still at the same time, the detective also said two-thirds of all the hits he had were 14- and 15-year-olds, the most gullible, if you will.

MR. ANGUS. Well, the second part of the question that you asked, Congressman, was the accessibility to those 14- and 15-year-olds of the older users and we have implemented a feature that now requires that anyone 18 or over know the exact email address or first and last name of the user to identify that user and invite them to be a friend.

MR. STUPAK. When did that start?

MR. ANGUS. That was announced I believe last week as part of our recent safety announcements.

MR. STUPAK. Okay. Because I was looking at some cases here, about four, five, six of them, that certainly were not--am I over time?

MR. ANGUS. Yes, that is a relatively new feature.

MR. STUPAK. Thanks.

MR. WHITFIELD. Thank you, Mr. Stupak. At this time I recognize Dr. Burgess.

MR. BURGESS. Mr. Kelly, you talked about some of the technologies that are employed by Facebook and you referred to segmenting and you alluded to other technical devices that you have for online protection. Can you fill us in on some of those others?

MR. KELLY. Sure. I mean, I want to highlight the fact that what we are trying to do is leverage social norms in the technology as well with the authentication, with the segmentation of the networks. The other factors--we don't like to talk a lot about the particular factors that we use to determine inappropriate usage because it may in fact lead people to try to get around them, but one of the ones that I talked about was number of rejected friend requests is the easiest thing. If somebody were to get on the network and try to become friends and thus get access to profiles of especially a bunch of high school students, that is something that we have a tool that runs every 4 hours and will flag that and it gets emailed to an engineer and we review that constantly every 4 hours, and we can research any inappropriate activity like that. It gets sent to our customer service team if that security engineer believes that it indicates a true complete misuse of the site.

MR. BURGESS. And these are individuals that have had some specific training in identifying aberrant behavior? They have had some law enforcement training? What--

MR. KELLY. They haven't had law enforcement training but they are highly technical engineers who have helped design the site.

MR. BURGESS. And I don't quarrel with the fact that you are all very bright and you have set up wonderful entrepreneurial businesses which epitomizes the American way, but you have seen, if you have followed any of these hearings, the enormity, the magnitude of the problems that we are up against and the devastating effect it is having on the next generation of Americans and it is certainly incumbent upon us while we celebrate your successes. We do want to ensure that the proper safeguards are in place for children who might access these sites, so is there any industry standard that says your safety engineers, if that is the correct terminology for that position. Are there any performance guidelines that they have to meet? Is there any special training that they



have to take--I really ought to ask the same question of whoever is sitting at the table.

MR. KELLY. We have written technology specifications for these tools and we are constantly upgrading them. We at Facebook have done this, and they are designed with my input--

MR. BURGESS. Let me just--

MR. KELLY. --the input of--

MR. BURGESS. I don't mean to interrupt you because I know what you have to say is important but have you monitored these hearings as we have been going through them the past several weeks?

MR. KELLY. Yes.

MR. BURGESS. You just can't help but be impressed by the enormity of the problem and how clever the criminal mind is. You know how clever the adolescent mind is at defeating whatever safeguards you are going to put up there but how clever the criminal mind is. We have seen a little bit of it in these public service announcements, but they hardly do justice to how clever these individuals are, and at one point in Justin Berry's testimony, the comment was made, "We laugh at people who try to stop us, we are so much smarter than they are." So my question to you again is, what training and what safeguards, what industry standards are there? If there are not any, do you think we should develop some?

MR. KELLY. There are not currently industry standards focused on these sites, in large part because--

MR. BURGESS. On safety officers.

MR. KELLY. Around safety officers, but in large part because--

MR. BURGESS. What about at MySpace?

MR. ANGUS. We train all of our employees who are responsible for safety and security on our practices. We have also reached out to the other social networking sites to try and establish best practices and we are engaged in that dialogue.

MR. BURGESS. And do they have training from law enforcement? Do they have training from people who specifically prosecute these types of crimes so they know what to look for?

MR. ANGUS. Yes, Congressman, we do speak regularly with law enforcement. Our chief security officer is a former U.S. prosecutor and was formerly with the Los Angeles District Attorney's Office and is familiar with the needs of law enforcement in their prosecutions. We work with them regularly.

MR. BURGESS. You made the statement to Mr. Stupak that no one under 14 is allowed on MySpace.

MR. ANGUS. That is correct.

MR. BURGESS. Have you ever known anyone to mislead someone about their age?

MR. ANGUS. Certainly.

MR. BURGESS. And so what are you doing now to prevent that from happening?

MR. ANGUS. When we find out that someone is misrepresenting their age, they are--

MR. BURGESS. These are kids. They are so clever. How are you going to find out?

MR. ANGUS. They are clever. It is our part of the education process. We believe that educating parents and the students--

MR. BURGESS. How long is that process going to take?

MR. ANGUS. We have a parents' guide that will be released prior to the end of--before the beginning of the school year.

MR. BURGESS. I referenced it earlier, I applaud and welcome the public service activities that you have going on but I have just got to tell you, I think that all of us are way behind the curve on this and playing catch-up in a disease, and I will use that term, that is exploding exponentially, it is not a good feeling for me sitting on this side of that table about where we are in the trajectory of trying to get a handle on this problem.

MR. ANGUS. I share your--

MR. BURGESS. Let me just ask you one other thing. Now, no one under 14--we heard--our initial witness in this whole series of hearings was someone who started when they were 14. As far as I can tell, his life has been seriously derailed by activities on MySpace. I realize your corporation did not own it at the time but do you think 14, is that an adequate safeguard to place on MySpace?

MR. ANGUS. We believe that it is. Again, we believe that the 14-year-olds are going to join and we employ security measures specifically for the 14- and 15-year-olds that we believe better protect them and--

MR. BURGESS. Now, these--

MR. ANGUS. --empower them.

MR. BURGESS. --would not have been in place when Mr. Berry began his career on MySpace, or--I beg your pardon. I am--

MR. ANGUS. But if I may, you asked about our coordination with law enforcement. I testified at California State hearings, and one of the things that I heard from a lieutenant who was operations commander for ICAC Task Force in northern California was very troubling to me, that the laws in many States are not consistent and do not permit law enforcement to go after some of these online predators. The act of a predator engaging in an online sexual discussion may in and of itself not be enough to warrant prosecution, and it is this kind of activity that should be criminalized.

MR. BURGESS. How much time do you give yourself to evaluate the information that you are given by new subscribers? If someone goes online and says I want to have a spot on MySpace, I am 14 years old, here is my information, is it immediate hookup that they have or do you delay that by a little while so you can check the information?

MR. ANGUS. It is immediate. If they enter in the information, if the information is correct, they have an account and they begin setting up that account.

MR. BURGESS. What would be the problem with perhaps delaying that by some period of time to allow the information to be verified?

MR. ANGUS. If they--I am at a loss--

MR. BURGESS. If someone comes to MySpace and says I am 14 years old, I want a site, provides you whatever information is required to set up a set for a 14-year-old, what would be the problem in delaying the immediate setup of that site and allowing your cyber detectives time to verify that that information is in fact correct, that this 14-year-old is not in fact a 28-year-old?

MR. ANGUS. Congressman, right now--

MR. BURGESS. Or that this 14-year-old is not in fact a 10-year-old?

MR. ANGUS. Congressman, right now we don't have any means to verify the information that is provided to us.

MR. BURGESS. How--

MR. ANGUS. If they provide a correct--

MR. BURGESS. If I could, how many people are going to sign up to MySpace today?

MR. ANGUS. Probably roughly 250,000.

MR. BURGESS. And how many of those will be 14 years of age?

MR. ANGUS. I don't know the answer to that question, Congressman. I do know that roughly 20 percent are under the age of 18.

MR. BURGESS. And that is a figure that could be verified if someone were to look at your records--

MR. ANGUS. That--

MR. BURGESS. --so that there wouldn't be someone who says they are 16 who is in fact 60?

MR. ANGUS. These are numbers actually that are reported to us by comScore Mediametric, so it is a third party who provides the ages of those users.

MR. BURGESS. Well, let me ask you a question, and I apologize for linking your site with the witness we had at the very beginnings of these hearings, but as that individual testified to us, and I am not a big person on liability. In fact, I am probably on the other side of that equation but I couldn't help but think that some site somewhere might have enormous

liability because of what has happened to this young individual. Do you all concern yourselves with the fact that if someone gets injured using your product in a way that maybe it wasn't intended but basically conforms to the rules and they get injured, do you incur any type of liability from that?

MR. ANGUS. Congressman, I wouldn't want to comment on any pending litigation--

MR. BURGESS. I wouldn't expect that you would.

MR. ANGUS. We are deeply concerned that if anyone--

MR. BURGESS. I would really like for all three of you if you don't mind, because I am going to run out of time here in just a moment, if there is some way with your various legal departments if you would just explore that, how do you in fact see yourselves as protected from--we saw the PSA run in reverse up there. If that situation happens and that child is critically injured or killed, how do you protect yourselves from liability if you have been the conduit to bring the predator and victim together? Is there liability there? I honestly don't know. I am not a lawyer. I don't know legal theory. It would seem to me if we have got those warnings on the package of cigarettes that there may be some clever lawyer somewhere in this country who would try to draw a straight line between those two dots. Mr. Chairman, you have been very indulgent.

MR. KELLY. First of all, the harm to the child is obviously our first concern, not liability, but in the design of the site, we figure if there are best practices in place that proper usage, that the best standards should in fact govern the possible interaction between kids and adult predators, which is why we separate the sites. I want to add one thing on the standards question that you have asked, and I spent the day yesterday with the National Association of Attorneys General and I would add for the committee's consideration that the National Association of Attorneys General has asked Facebook to submit its security standards for consideration as a best practice as they go forward in their deliberations about how they are going to set these standards.

MR. BURGESS. And I would agree with the gentleman that the safety of the child is the first concern but what we have seen over the past several weeks is the enormity of the pressure put on the rest of society by the predator community and the Internet has boosted that, has turbocharged that to a degree that I don't think I am alone on this committee, I was absolutely unaware as to the dangers that were out there with these types of sites. Again, I welcome the entrepreneurship that you bring to the American culture, the things that you are able to provide society but do understand that we on this side do feel an

obligation to put the proper boundaries around this so that our next generation of Americans is protected.

MR. KELLY. And we deeply share those concerns and that is why we built them into the technology.

MR. WHITFIELD. Ms. DeGette, you are recognized for 10 minutes.

MS. DEGETTE. Thank you, Mr. Chairman. Let me say, I actually agree with the detective and I agree with what you gentlemen are saying in terms of you don't want to put so many restrictions on these sites that you drive kids to other places where they may not have scrupulous oversight and I really agree with that and that is one reason I agree with this thing about having 14- and 15-year-olds in a segregated site or not letting them be on sites like MySpace. I also worry that predators could then know exactly where to go and zero in to kids if you have sites just for those, but having said that, I think that everybody in this room would agree, we need to work harder as a community, that you and similar companies need to work harder and smarter to try to thwart these predators and we need to figure out if there is a--well, for Congress. Just quickly, would you agree with that, Mr. Kelly?

MR. KELLY. I am sorry. Could you repeat--

MS. DEGETTE. Would you agree with the fact we all need to work harder--

MR. KELLY. Oh, absolutely, at all levels.

MS. DEGETTE. And Mr.--is it Hiler or Hiller?

MR. HILER. Yes, Hiler.

MS. DEGETTE. Would you agree with that too?

MR. HILER. Yes.

MS. DEGETTE. Would all of you agree with what the detective was saying about parents need to take a role to look at their child's contacts on the Internet and to take an active role?

MR. KELLY. Absolutely.

MR. ANGUS. Parental involvement is one of the best things that we can do to enhance safety.

MS. DEGETTE. Mr. Hiler?

MR. HILER. Absolutely.

MS. DEGETTE. Now, Mr. Angus, I want to ask you, and I just want to be really frank here because as I said earlier, you were here when I was talking earlier, there is really no way to verify if a 12-year-old is registering a birth date that says they are 16, is there?

MR. ANGUS. That is right.

MS. DEGETTE. As you said, you can go and if they try to back up and redo the--

MR. ANGUS. You can--

MS. DEGETTE. But the 12-year-olds--I am telling you right now because I have watched it personally with my eyes, I watched an 11-year-old sign up--that would be my daughter--for a MySpace site, and you know that is happening, right?

MR. ANGUS. They can do it.

MS. DEGETTE. And it is happening, and you don't have a way to stop that really, do you?

MR. ANGUS. We are doing everything that we can including updating those search algorithms and again, it is our belief--

MS. DEGETTE. Actually, there is more you could do because Mr. Kelly is doing some of it although his site is so restricted anyway because of the way they sign users up but you can do algorithms that will go beyond just the date of birth that they register to start to weed out some of the underage users.

MR. ANGUS. Oh, yes. Our--

MS. DEGETTE. And are you working on that?

MR. ANGUS. The algorithms that I spoke of actually scan not just the user information that the users input when they register but all of the text that they put on their site.

MS. DEGETTE. And is that vigorously done?

MR. ANGUS. Yes, it--

MS. DEGETTE. And how many people are screened out every week because they are underage using those algorithms?

MR. ANGUS. I don't know the weekly number. I know that over 200,000 have been removed from the site and I--

MS. DEGETTE. Since when?

MR. ANGUS. I don't know the answer to that.

MS. DEGETTE. Mr. Chairman, I would ask unanimous consent Mr. Angus be allowed to supplement his testimony.

MR. WHITFIELD. Without objection.

MS. DEGETTE. Thank you.

MR. ANGUS. Thank you.

MS. DEGETTE. Now, I would ask you, Mr. Angus--all three of you testified that your customer service personnel take complaints of child pornography and other inappropriate actions but I would ask you, Mr. Angus, would you object if we could figure out which regulatory agency could take those complaints and if they were adequately funded either by a government-industry consortium or some other way--I really--I am very intrigued with what the U.K. and Australia do where they have the little link right on their website where the report can go to an experienced law enforcement agency. Would you agree and participate in helping us find a way to do that kind of reporting?

MR. ANGUS. We would welcome that, yes.

MS. DEGETTE. And Mr. Kelly, would you?

MR. KELLY. Yes, we would welcome that.

MS. DEGETTE. And what about you, Mr. Hiler?

MR. HILER. The same.

MS. DEGETTE. Now, I just think that way you don't have to have recent college graduates who are really there for consumer protection to be making law enforcement decisions, right?

MR. HILER. Um-hum.

MS. DEGETTE. Okay. Mr. Hiler, I want to ask you a couple of questions because you testified that your company has recently decided to keep all IP addresses for users that are on your site, correct?

MR. HILER. Just to clarify, we have since the beginning of the site to my knowledge always retained the IP address upon registration.

MS. DEGETTE. And are you keeping any other IP information?

MR. HILER. We are now working with the National Center to establish what other IPs might be useful for them in the cyber tip line reporting and law enforcement in general.

MS. DEGETTE. Okay. And you are going to store the data indefinitely?

MR. HILER. All IP registration data that we store, we will retain and preserve indefinitely.

MS. DEGETTE. And why do you do this?

MR. HILER. We are deeply committed to helping law enforcement. One of the things that the National Center has pointed out is that if we give them the IP address of a member who has uploaded child porn and the IP address is above a certain amount of months, it may not be useful to them for some of the reasons that were cited in yesterday's hearing and so if we can get a fresh IP, that is absolutely critical to law enforcement.

MS. DEGETTE. And when are you talking about that fresh IP, what you mean is when they upload a photograph?

MR. HILER. Yes. So now for every--

MS. DEGETTE. That is what you are keeping as well?

MR. HILER. In just a few days every photo uploaded is going to have an IP address associated with it.

MS. DEGETTE. And you will save that data as well as the initial user--

MR. HILER. Absolutely. We will save that indefinitely.

MS. DEGETTE. Okay. And do you know how much it is going to cost you do to that?

MR. HILER. I don't know. We store vast amounts of photos. That costs a lot of money. Sticking on an IP address, I can't imagine that is going to be a huge portion of the cost.

MS. DEGETTE. Mr. Kelly, you are nodding your head. Do you--

MR. KELLY. We tag--every photo on Facebook is connected to a user account at this point so there is a direct connection there, and I would be surprised if adding an IP address to those pieces of information. We have it currently in our logs. It probably wouldn't make it--

MS. DEGETTE. How long do you retain that IP--

MR. KELLY. Indefinitely.

MS. DEGETTE. Indefinitely. And Mr. Hiler, you get subpoenas for this information from law enforcement agencies, correct?

MR. HILER. We do get subpoenas.

MS. DEGETTE. And how often do you get those subpoenas?

MR. HILER. Not as often as--we have a strong safety record. A couple a month perhaps.

MS. DEGETTE. And you compile them within one to two days. Is that correct?

MR. HILER. If not faster.

MS. DEGETTE. Okay. Do you ever get subpoenas, Mr. Kelly?

MR. KELLY. Yes. We get about two to three a week.

MS. DEGETTE. Two to three a week, and how quickly do you comply?

MR. KELLY. We comply as quickly as we can, usually within 24 to 48 hours.

MS. DEGETTE. Do either one of you gentlemen think that it would be overly burdensome--from what you know about your business keeping this IP address information, not even the photographs but just the addresses, do you think it would be overly burdensome for Congress to make a rule that says that ISPs would have to keep that information for 1 year?

MR. KELLY. The only concern I would put out there is the idea that the technology would get ahead of the law but as a best practice, I don't have a problem with that.

MS. DEGETTE. Mr. Hiler.

MR. HILER. Thank you. Yes. In our case, we own our own technology platform so for us to add a point at which we capture IP is a fairly trivial matter. For ISPs, from what I understand, this sort of IP collection is not baked into the technology so--

MS. DEGETTE. But they keep that information now.

MR. HILER. I don't--

MS. DEGETTE. They told me they keep it now.

MR. HILER. They keep the IP--

MS. DEGETTE. The only question is, how long do they keep it for. They keep the IP addresses though.



MR. HILER. Of the photos that are uploaded?

MS. DEGETTE. They don't--they--yes, they do.

MR. HILER. Okay. My understanding was that the ISPs retain and preserve the IPs of all visitors, and so for them, that is much more onerous and burdensome preservation request.

MS. DEGETTE. But they already do that.

MR. WHITFIELD. I didn't understand that they kept the photos.

MS. DEGETTE. No, but when people turn on their computers or upload information and if there is a new IP address generated, then they keep that as well. Mr. Angus, I didn't mean to leave you out.

MR. ANGUS. Thank you.

MS. DEGETTE. How long does your company retain this information?

MR. ANGUS. As a media--

MS. DEGETTE. The address.

MR. ANGUS. As a media company, Fox is very supportive of data retention. It helps us to police piracy. We retain IP addresses associated with registrations indefinitely and we retain IP addresses associated with all other communications on our site for at least 90 days.

MS. DEGETTE. Okay.

MR. ANGUS. And we work with law enforcement, and if law enforcement sends us a preservation request in connection with an investigation, we will preserve that information indefinitely pending--

MS. DEGETTE. Right, and you know, the thing is, the preservation requests are different from subpoenas for IP addresses because the preservation requests are when they see the activity going on. Later on they might need to find out where a perpetrator is and subpoena that address.

MR. ANGUS. Yes.

MS. DEGETTE. And do you have any idea how much it would cost your company to preserve those IP addresses for 12 months instead of 90 days?

MR. ANGUS. I don't, but again, the IP logs are such a small amount of data that I can't imagine that it would be cost prohibitive but--

MS. DEGETTE. Yes, I can't either.

MR. ANGUS. --it is something that we are certainly willing to explore.

MS. DEGETTE. Okay. Thank you very much, Mr. Chairman.

MR. WHITFIELD. Thank you. At this time I recognize the Vice Chairman of the committee, Mr. Walden.

MR. WALDEN. Thank you very, much, Mr. Chairman. Mr. Angus, I want to go through on MySpace.com, kind of how this works, and

following up on what some of my colleagues have already asked. First of all, it is up to the person registering to tell you how old they are, right?

MR. ANGUS. That is correct.

MR. WALDEN. Which is the equivalent of going to the liquor store without ever having to show ID and say I am 21 when you are 18, not that anybody has ever done that, least of all Dr. Burgess.

MR. BURGESS. I certainly haven't.

MR. WALDEN. But it is in effect a self-reporting mechanism, right?

MR. ANGUS. That is correct.

MR. WALDEN. And you don't have, and I assume your colleagues don't have any real ability to determine to say to that registrant, show me your ID, show me your age.

MR. ANGUS. That is really the issue we are faced with is that age verification really amounts to identity verification and there is no viable means for us to do that today.

MR. WALDEN. Now, you could do that if you required some sort of credit card, a nominal 50-cent charge or something because most credit card companies don't issue credit cards to those under 18.

MR. ANGUS. It would amount--it would allow--well, I think first of all, some of them do issue credit cards these days to very young users surprisingly and--

MR. WALDEN. But that is going to be a small--

MR. ANGUS. In addition, I think it is also very easy for users to get access to a credit card, especially if we are talking about a nominal fee, and I fear that again we are--

MR. WALDEN. Well, but let us go back to--we are trying to find ways to give you the ability to ID somebody based on age. I mean, as a parent of a teenager, you can download songs off iTunes but it kind of needs the wallet needs a credit card, and that is true on other purchases, which involves the parents, at least in our household, and so I am just trying to figure out how you got there. There is nothing that stops a young person from using a pseudonym. "I am Mike Burgess and I was born in 1988 and I am 18," right. Now, do you link that name and that age to the--do they have to list an email address?

MR. ANGUS. They do provide an email address with registration.

MR. WALDEN. And that is a requirement?

MR. ANGUS. Yes.

MR. WALDEN. It is a requirement. So you link that email address to that name and to that date of birth?

MR. ANGUS. That is correct.

MR. WALDEN. What if they come back later using the same email address but show up as a different name and a different date of birth? Do you track that?

MR. ANGUS. My understanding of our site functionality is that you can only register once with an email address.

MR. WALDEN. They can go to Yahoo! and create a new email or go to another ISP.

MR. ANGUS. Exactly. That was where I was going, Congressman, is that there are--

MR. WALDEN. Just create a new name.

MR. ANGUS. That is certainly very easy these days to create numerous free Internet email accounts.

MR. WALDEN. You testified that your algorithms and other work, as laudable as it is, has identified 200,000 people you believe and removed them from your system.

MR. ANGUS. Correct.

MR. WALDEN. We don't know the timeline under which that has occurred?

MR. ANGUS. That is right.

MR. WALDEN. But somewhere that has happened, 200,000. You also, if I heard you correctly earlier in testimony, said there are 250,000 people registering today on average on MySpace.

MR. ANGUS. Yes.

MR. WALDEN. So you are actually targeting--your algorithms have identified very few people to kick off the system for being underage, right?

MR. ANGUS. Again, Congressman, I believe that that 200,000 figure is probably quite old at this point so again, I would appreciate the opportunity to supplement my testimony with more relevant and fresh data.

MR. WALDEN. Okay. That would be real helpful, especially in the context of today's hearing to know if your algorithms work. That would seem to me to be a pretty basic number we should get, so that would be most helpful. In terms of--well, I have talked obviously to some kids, some friends of my own son and, they just sort of laugh at the notion that any of them--that they somehow would get caught for saying they are a certain age when they are not. Do you find that as you--I mean, do all of you find that among teenagers? I mean, do any of them take this seriously, and should they? Fundamentally, is there any reason they should take this seriously?

MR. KELLY. We have the different authentication token, the invitation that you get to get authenticated into a high school network and in the neighborhood watch associated with that so our expectation of our users is that they will be interacting with students who are in the real world around them and so they do in fact take it seriously. I would encourage all of the members to talk to their young staff who are recent

college graduates about the difference that Facebook has made on college campuses, and now it is beginning to have the same difference on high school campuses.

MR. WALDEN. Right. Actually, I have heard about your service and in the context of younger people and they tell me the same thing, that it is a whole different deal, and I am not criticizing what you all do. I think we are all struggling with how do we protect our kids from the kind of violent encounters that are occurring every day in America in neighborhoods like ours with people that we could pass in the hall today. How do we do that together? And that is why we are probing so hard here, I think, is that what you are telling me is, Mr. Angus, you can't tell a 14-year-old from a 40-year-old.

MR. ANGUS. Well, Congressman, one of the things that you mentioned is that we do require an email address to register for the site. One of the things that we have been discussing internally is whether it would be possible to create a national registry of email addresses for convicted sex offenders and whether that is something that could be maintained as a database against which we could check registrants and screen them out from the service entirely.

MR. WALDEN. And while I don't want to take away from brainstorming techniques, nothing stops them from going to a free service and just getting a different email account.

MR. ANGUS. Well, if we criminalize that, then there are ramifications.

MR. WALDEN. Yes, I mean, but perverted acts somewhere are also criminal and if they are going to chase down kids and do horrible things to them, they are probably not going to hesitate going to Hotmail and getting a new email address, with all due respect. I appreciate what you are trying to get to. I think we are all saying, how do you do that? Maybe a registry gets you there, but I don't know. It is just--that is a good question. That is why you have staff. Do any of you check against any kind of sex offender registry today to see if they have spaces?

MR. ANGUS. We don't. The numerous registries aren't readily available to us. It is not something that we--

MR. WALDEN. Isn't that available through law enforcement? In some States they are public, I am told. Could we suggest that maybe you incorporate that in as you plan in the future?

MR. ANGUS. I don't believe they include email addresses but I could be wrong. I mean, to the extent that they do and they are required to register those, I--

MR. WALDEN. What if they include name and address? Don't you require that?

MR. ANGUS. Yes, we do, not address but name.

MR. WALDEN. So the extent at least they are dumb enough to use their real name--

MR. ANGUS. Certainly. If someone were to use--

MR. KELLY. That is the problem, Congressman, is that the likelihood that they will use their real name on an open service is very low.

MR. WALDEN. So that gets back to my point about if they are going to do illegal acts with a minor, they are going to get a different email address to. But at least you might catch--I mean, after what we saw yesterday from Chris Hansen on how this one fellow shows up twice to the same scam, I believe some of these guys are stupid enough to use their real name probably and their email address, and if you weed out one--

MR. ANGUS. Yes.

MR. WALDEN. I mean--

MR. ANGUS. If we could create a national registry, I think that would make it even better for us.

MR. WALDEN. Well, that is something we will take into consideration, but certainly I would think as you incorporate in other data and connect up with law enforcement, it would be an easy question to ask each law enforcement agency with whom you work, do you have a list, can you give us names, we will run them through our check. I mean, if you are checking for amount of skin in an image and that sort of thing and however your logarithms work, you think you ought to check, John Doe, who happens to be a sex offender, against it and weed them out. It is just real troubling what we have seen and learned and all that, and we are going to put pressure on organizations like yours because bottom line, you are in it to make money or Fox wouldn't have bought you, or I guess you are now Newscorp's or--I mean, these are money-making enterprises or you wouldn't be here, and as a result, there is an obligation to try and make them safe and we have an obligation to work with you to achieve that common goal and not to end up chasing people off into completely irresponsible sites. We recognize the boundaries. So I appreciate you being here today and the work you are trying to do to get there. We've just got a ways to go.

MR. ANGUS. Thank you, Congressman.

MR. WHITFIELD. Thank you. Dr. Burgess, I understand you have another question.

MR. BURGESS. Just if I might, Mr. Chairman. To all three on the panel, do you have a concept of the number of cases you have referred to law enforcement from kids clicking on an icon on your site and reporting aberrant behavior?

MR. ANGUS. I would want to reserve the right to supplement the record.

MR. BURGESS. And if we--

MR. ANGUS. From my memory, it would be probably about 100.

MR. BURGESS. And how many prosecutions from those referrals?

MR. ANGUS. Actually it depends on if you count cases in which we have participated or cases in which we have directly referred. There have been--I actually don't know the number of prosecutions that have resulted.

MR. BURGESS. If you wouldn't mind asking your department, Mr. Angus.

MR. HILER. I likewise would like the opportunity to supplement.

MR. BURGESS. And just so that we have some context within which to put it, you sign up 250,000 new members a day and have how many active members on your site?

MR. ANGUS. Over 85 million.

MR. BURGESS. And Mr. Kelly, you referenced eight million but I suspect the number is larger now?

MR. KELLY. We have eight million, just over eight million registered users and growing quite rapidly every day.

MR. BURGESS. Yes, and if I do my math right, that is one customer service representative for every 475,000 people?

MR. KELLY. Um-hum. It is like a Congressman representing--

MR. BURGESS. Yeah. Got you. Mr. Hiler, how about yourself? Do you know the number of cases you have referred to law enforcement?

MR. HILER. I don't. I can tell you that we have reported several hundred cases to the National Center and the cyber tip line, and we have 27 million members on our site roughly, and I can get back to you on the number of cases we have referred to law enforcement but also that we have processed.

MR. WHITFIELD. You all can provide that for the record.

MR. BURGESS. With nearly 100 million registrants between the three of you, has there been one case prosecuted that any of you are aware of?

MR. ANGUS. We know of a couple of cases that have been prosecuted.

MR. BURGESS. And you will provide us that information as well?

MR. ANGUS. We participated in a number of prosecutions and I am not sure whether they have resulted from proactive referrals or contact from law enforcement.

MR. BURGESS. Very good. And just one last question, Mr. Kelly. Do you feel like you have been adequately responsive to school if there are sites that the kids might use for bullying? One of the issues, particularly as you get into the high school level but I guess it could

happen in college as well, the peer pressure groups and the bullying activities, do you adequately police for that as well?

MR. KELLY. We are very concerned about that and where it is a violation of our terms of service and of our community standards to launch a hate site against an individual or against a group and we take those down as quickly as we find them.

MR. BURGESS. And how would you rate your responsiveness to schools in general?

MR. KELLY. I would rate our responsiveness as very good.

MR. WHITFIELD. The gentleman's time has expired.

MR. BURGESS. Thank you, Mr. Chairman.

MR. WHITFIELD. We have to move on. Thank you all very much for your testimony, and our staff will be back with you on the information that we requested. At this time I would like to call the third panel: the Honorable Pamela Jones Harbour, who is Commissioner of the Federal Trade Commission, Mr. Diego Ruiz, who is the Deputy Chief, Office of Strategic Planning and Policy Analysis, Federal Communications Commission, and the Honorable Richard Blumenthal, Attorney General of the State of Connecticut. Thank you all very much for being with us this afternoon and for your patience. As you know, this is the Oversight and Investigations Subcommittee. We do take testimony under oath. Do any of you have difficulty in testifying under oath? Okay. Do any of you desire to be represented by legal counsel? Okay. Raise your right hand.

[Witnesses sworn.]

MR. WHITFIELD. Thank you very much. You are under oath now, and Commissioner Harbour, we recognize you for your 5-minute opening statement.

**STATEMENTS OF THE HONORABLE PAMELA JONES HARBOUR, COMMISSIONER, FEDERAL TRADE COMMISSION; DIEGO RUIZ, DEPUTY CHIEF, OFFICE OF STRATEGIC PLANNING AND POLICY ANALYSIS, FEDERAL COMMUNICATIONS COMMISSION; AND THE HONORABLE RICHARD BLUMENTHAL, ATTORNEY GENERAL, STATE OF CONNECTICUT**

MS. HARBOUR. Thank you, Mr. Chairman, Ranking Member Stupak, and members of the subcommittee.

I thank you for holding this hearing today on a very important topic, making the Internet safe for children. I also appreciate the opportunity to discuss the Federal Trade Commission's efforts to help parents and

children understand and manage the risks of social networking sites on the Internet.

The Internet has revolutionized the way that people communicate with each other. Email, chat rooms, and instant messaging are just a few of those ways. Today's social networking sites are the next generation in communications technology. Children have enthusiastically and passionately embraced this technology. MySpace, as we have heard, and Facebook reportedly rank among the top ten websites among young people ages 12 to 17. Social networking sites provide these young people with a forum to express themselves creatively, exchange ideas or make new friends across the country and around the world. Like other activities on the Internet, however, social networking sites pose risks to children. In particular, sexual predators may use the information that children provide on these sites to identify, contact, and exploit them. These significant risks and opportunities require a whole new entry in the book of parenting.

The Federal Trade Commission is extremely committed to helping create a safer online experience for children through consumer education and targeted law enforcement. In May the FTC released two user-friendly consumer education brochures. The first is directed to parents. It describes in non-technical terms what social networking sites are, how they can pose risks to children and how parents can monitor what their children are doing in cyberspace. For example, the publication encourages parents to keep their computers in a common area in the home and to encourage the use of privacy settings that restrict who can access their children's sites.

The second FTC publication is directed to teens and tweens. Tweens are children between the ages of eight and 12. The brochure counsels children to think about how a social networking site works before they decide to join it. For example, some sites limit access to a defined or closed community of users. The publication also warns children never to post information that can be used to locate them or steal their identities such as their full name, their address, or phone number and above all, children must know that engaging in risky behavior online can have serious, even deadly consequences offline.

The FTC's consumer information on social networking sites is also featured prominently on OnGuardOnline.gov. This is an innovative, multimedia website designed to educate consumers about basic computer security practices. OnGuardOnline offers information and guidance on social networking sites, wireless security, identity theft, and more. It also includes a video for parents on teaching kids online safety. OnGuardOnline has been enormously successful, attracting between 6,000 and 7,000 unique visitor hits each day in the past 2 months alone.



I am pleased that Comcast.net, Verizon DSL, TRUSTe, many Members of Congress, and at least seven of the social networking sites that are most popular with teens have already provided links to the FTC materials. We encourage businesses everywhere to use these materials to raise awareness among their customers.

In addition to providing critical consumer education materials, the FTC enforces the Children's Online Privacy Protection Act, or COPPA. Congress enacted COPPA to prohibit unfair or deceptive practices in the collection, use, or disclosure of personally identifiable information from and about children on the Internet. The law gives parents the power to control whether information is collected online from their children under 13 and how this information may be used. Website operators must take several affirmative steps before collecting, using, or disclosing personal information from a child. Operators must provide their privacy policies to parents. They must obtain verifiable consent from a parent or a guardian before collecting the personal information from a child, and they must maintain reasonable procedures to protect that information. The FTC staff is currently investigating several social networking sites to determine whether these sites are in compliance with COPPA.

And in conclusion, consumer, government, advertisers, and technology companies all have a shared interest and responsibility in creating a secure online environment. The Federal Trade Commission is committed to the important work of safeguarding children's information online and educating consumers about the risks involved in social networking. We look forward to working with members of this subcommittee to provide greater security and privacy for American consumers. Thank you.

[The prepared statement of the Hon. Pamela Jones Harbor follows:]

PREPARED STATEMENT OF THE HON. PAMELA JONES HARBOUR, COMMISSIONER, FEDERAL  
TRADE COMMISSION

Mr. Chairman, Ranking Member Stupak, and members of the Subcommittee, I am Pamela Jones Harbour, a Commissioner at the Federal Trade Commission ("FTC" or "Commission").<sup>1</sup> I appreciate this opportunity to discuss the Commission's efforts to help ensure that parents and children understand the risks of social networking websites and the steps they can take to reduce these risks before participating on such sites.

---

<sup>1</sup> This written statement reflects the views of the Federal Trade Commission. My oral statements and responses to any questions you may have represent my own views, and do not necessarily reflect the views of the Commission or any other individual Commissioner.

## I. Introduction

Technology constantly changes the ways that consumers can communicate with each other. The telephone was the primary technology consumers used to converse for most of the last century. During the 1980's and the 1990's, personal computers and the Internet vastly expanded the options available for consumers to communicate with each other – email, chat rooms, online bulletin boards, and instant messaging, to name a few. Social networking websites<sup>2</sup> are the next generation in communications technology, providing a platform for multi-faceted communication between participating users.

Children, especially teens and tweens,<sup>3</sup> have embraced this online technology. According to a 2005 report by the Pew Internet and American Life Project, 87% of children between the ages of 12 and 17 are online, and approximately 11 million of them access the Internet every day.<sup>4</sup> Teen use of social networking websites in particular has exploded recently. MySpace and Facebook reportedly rank among the top ten websites among children age 12 to 17, based on the average minutes they spent online.<sup>5</sup>

At the same time that social networking websites offer online communication, camaraderie, and community among teens and tweens, they, like other activities on the Internet, also can pose risks. Because the information that children post on their online journals, web logs or “blogs” can be accessed by other Internet users, social networking websites raise heightened privacy and security concerns. In particular, sexual predators may use the information that children provide on social networking sites to identify, contact, and exploit them,<sup>6</sup> unless these sites are constructed to reduce access to this information, or users themselves take steps to limit unwanted access.

The Federal Trade Commission is committed to helping create a safer online experience for children. I will discuss in more detail the agency's efforts to help protect children through consumer education and targeted law enforcement. In addition, I will discuss the need for social networking websites – individually, collectively, and, most importantly, expeditiously – to develop and implement safety features to protect children who visit their sites and empower parents to protect their children when they do so.

## II. Consumer Education

In response to the rapid increase in use of social networking sites by teens and tweens, one element of the FTC's “safe networking” program has been to develop user-friendly consumer education materials, both for parents and for children. Last month, the agency posted on our website two consumer publications providing practical guidance to parents, teens, and tweens about using social networking websites safely.

### A. Advice for Parents

It is, of course, critically important for parents to know what their children are doing in cyberspace. Accordingly, one of the FTC's publications is directed specifically to

<sup>2</sup> Social networking sites host weblogs, or “blogs.” A blog is a website where regular entries are made (such as in a journal or diary). Blogs often function as an online author's personal journal that also may contain hypertext, images, and links to video or audio files or other Web pages. See <http://en.wikipedia.org/wiki/Blog>.

<sup>3</sup> For purposes of this testimony, teens are children age 13 to 17, while tweens are children age 8 to 12.

<sup>4</sup> See Pew Internet & American Life Project Report, *Teens and Technology: Youth Are Leading the Transition to a Fully Wired and Mobile Nation* (July 27, 2005), available at [http://www.pewinternet.org/pdfs/PIP\\_Teens\\_Tech\\_July2005web.pdf](http://www.pewinternet.org/pdfs/PIP_Teens_Tech_July2005web.pdf).

<sup>5</sup> See comScore Media Metrix survey, *The Score: Teens Highly Engaged Online* (Mar. 16, 2006), available at <http://www.imediaconnection.com/content/8691.asp>.

<sup>6</sup> See, e.g., *Michigan Teen Home Safe & Sound: Authorities Say 16-Year-Old Flew To Mideast For 'MySpace' Rendezvous* (June 12, 2006), available at <http://www.cbsnews.com/stories/2006/06/09/tech/main1697653.shtml>; Tehani Schneider & Adam Teliercio, *Free Expression Blooms in Risk-laden MySpace*, *Morristown Daily Record*, May 14, 2006.

parents, and describes in non-technical terms what social networking websites are, how they can pose risks to children, and how parents can monitor their children's activities on such sites.<sup>7</sup> The publication encourages parents to keep their home computers in an open area, such as the kitchen or family room, so that they can see where their children go when they go online.<sup>8</sup> Parents should use the Internet with their children, and visit popular sites, including social networking sites if their children are using them. Parents should review the information their children post on blog sites,<sup>9</sup> and encourage the use of privacy settings to restrict who can access and post on their children's sites.

#### **B. Advice for Children**

Another FTC publication is directed to teens and tweens, and gives them important safety tips if they are using social networking sites.<sup>10</sup> The brochure counsels them to think about how a particular social networking website works before they decide to join. For example, some sites allow only access by a defined community of users. Others allow anyone and everyone to view their postings. If teens and tweens decide to join a particular social networking website, they should consider using the site's particular privacy settings to limit access to their postings.

Moreover, the publication warns teens and tweens to be cautious about the information they post. They should post neither information that can be used to locate them in the offline world (for example, they should not post their full name, address, phone number), nor information that could be used to facilitate identity theft. The agency also warns them that school admissions officers and potential employers may be able to look at their photos and postings. Finally, it warns that once information is posted online, it may be impossible to take it back. Even if the teen or tween deletes the information from his or her own site, older versions may still exist on other people's computers. Above all, children must know that engaging in risky behavior online (such as "flirting" with someone they do not know offline) can have serious, even deadly, consequences, and they should be wary about meeting in person someone whom they know only from the online world.

#### **C. OnGuardOnline**

The FTC's consumer information on social networking websites also is featured prominently on OnGuardOnline.gov, an innovative multimedia website designed to educate consumers about basic computer security practices. OnGuardOnline has become the hallmark of the Commission's larger cybersecurity campaign. OnGuardOnline is built around seven timeless tips about online safety.<sup>11</sup> In addition, the site hosts specific

<sup>7</sup> See FTC Facts for Consumers: Social Networking Sites: A Parents' Guide (May 2006), available at <http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.pdf>.

<sup>8</sup> A March 2005 report by the Kaiser Family Foundation found that 31% of 8 to 18 year olds have a computer in their bedroom, and 20% have Internet access in their rooms. See *Generation M: Media in the Lives of 8-18 Year-olds* (Mar. 9, 2005), available at <http://www.kff.org/entmedia/7251.cfm>.

<sup>9</sup> According to a recent study, sixty-one percent (61%) of teens reveal their contact information on their blogs by disclosing their email address (44%), instant messenger name (44%), or a link to a personal home page (30%). Fifty-nine percent (59%) reveal their location in terms of a city or state. Thirty-nine percent (39%) of teen bloggers provide their birth date, and twenty percent (20%) disclose their full name. See David Huffaker, *Teen Blogs Exposed: The Private Lives of Teens Made Public* (2006), available at [http://www.soc.northwestern.edu/gradstudents/huffaker/papers/Huffaker-2006-AAAS-Teen\\_Blogs.pdf](http://www.soc.northwestern.edu/gradstudents/huffaker/papers/Huffaker-2006-AAAS-Teen_Blogs.pdf).

<sup>10</sup> See FTC Facts for Consumers: Social Networking Sites: Safety Tips for Teens and Tweens (May 2006), available at <http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.pdf>.

<sup>11</sup> See <http://www.OnGuardOnline.gov>. The seven tips are described in detail in the FTC publication, Stop Think Click: Seven Practices for Safer Computing, available at <http://onguardonline.gov/stopthinkclick.html>. The seven practices for safer computing are: (1) Protect your personal information; (2) Know who you're dealing with; (3) Use anti-virus and anti-

information modules on topics such as social networking, wireless security, identity theft, phishing, spyware, and spam. OnGuardOnline features up-to-date articles from the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT), such as a newly added piece on the troubling practice of "Cyberbullying," that is, using technology to harass, or bully, someone else. There also is a video for parents on "Teaching Kids Online Safety."

In the past two months, OnGuardOnline has had between six and seven thousand unique visitors each day. In early June 2006, the FTC's social networking tips for parents and tips for teens and tweens were, respectively, the second and third most popular pages on OnGuardOnline, after the site's home page. Comcast.net recently promoted the social networking module as a "featured link," driving significant traffic to the website, and Verizon DSL's customer default homepage and TRUSTe link directly to the social networking module, as well.

OnGuardOnline was developed through a partnership with cybersecurity experts, consumer advocates, online marketers, and other federal agencies. It is a great example of public-private cooperation. The agency deliberately branded OnGuardOnline independently of the Federal Trade Commission to encourage other organizations to make the information their own and to disseminate it in ways that reach the most consumers.

Many of the social networking websites themselves have linked directly to the social networking module on OnGuardOnline. Thus far, eleven of the social networking websites most popular with teens either have already posted links to FTC materials or have informed our staff that they will do so in the near future,<sup>12</sup> and these links have directly contributed to the increased traffic at OnGuardOnline.

### III. Law Enforcement

Congress enacted the Children's Online Privacy Protection Act – or COPPA – to prohibit unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personally identifiable information from and about children on the Internet.<sup>13</sup> The statute gives parents the power to determine whether and what information is collected online from their children under age 13, and how such information may be used. COPPA, and its implementing rules, apply to operators of websites directed to children under the age of 13.<sup>14</sup> They also apply to operators of general audience websites who have actual knowledge that they are collecting personal information from children under the age of 13, which includes some social networking websites.<sup>15</sup>

---

spyware software, as well as a firewall, and update them regularly; (4) Be sure to set up your operating system and Web browser software properly, and update them regularly; (5) Protect your passwords; (6) Back up important files; and (7) Learn who to contact if something goes wrong online.

<sup>12</sup> The sites that have posted links to OnGuardOnline include: Alloy (<http://www.sconex.com/content/safety.php>); Buzznet (<http://www.buzznet.com>); Facebook (<http://www.facebook.com/help.php?tab=abuse>); Friendsorenemies (<http://www.friendsorenemies.com/about.php>); MyYearbook (<http://www.myearbook.com>); TagWorld (<http://tagworld.com/-/Main.aspx>); and Yahoo! 360 (<http://security.yahoo.com>). The sites that have informed FTC staff that they will post the materials are: HI5; Microsoft Spaces; MySpace; and Tagged.

<sup>13</sup> See Statement of Basis and Purpose, 16 C.F.R. Part 312.

<sup>14</sup> See Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6508, and the Commission's COPPA Rule, 16 C.F.R. Part 312.

<sup>15</sup> The Commission has brought two cases in which website operators were alleged to have had actual knowledge that they were collecting personal information from children under 13 on their general audience websites. See *United States v. UMG Recordings, Inc.*, Civ. No. CV-04-1050 JFW (Ex) (C.D. Cal. Feb. 17, 2004) (civil penalty of \$400,000); *United States v. Bonzi Software, Inc.*,

COPPA and its implementing Rule mandate that website operators take several affirmative steps *before* collecting, using, or disclosing personal information from a child under age 13. They must post on their websites a copy of their privacy policy. Operators also must provide parents with a notice describing their privacy policies. They must obtain verifiable consent from a parent or guardian before collecting personal information from children. And once operators have collected this information, they must establish and maintain reasonable procedures to protect its confidentiality, security, and integrity.<sup>16</sup>

The FTC staff currently is investigating several social networking websites to determine whether they are in compliance with COPPA and its implementing Rule.

#### **IV. Looking Ahead: Self-Regulation and Industry Best Practices**

Consumers, government, technology companies, and advertisers all have a shared interest and responsibility in creating a secure online environment. Social networking website operators are no exception.

The social networking industry has a clear incentive to create a safe online community. They owe this to their users, and sites that do not make online safety a priority may find it hard to compete with those that do. Some social networking websites already allow users to restrict access to the information they post, such as by creating sites with more closed, defined communities or enhancing specific privacy features on their sites.

Last week, two summits addressed issues posed by social networking sites, one hosted by the National Center for Missing and Exploited Children and the other hosted by WiredSafety.org. These summits focused, in part, on industry best practices. These meetings are positive steps to encouraging a meaningful industry response to the risks that social networking sites pose for children. The Commission hopes that the momentum from these summits continues to build so that industry best practices are developed and implemented as quickly as possible.

#### **V. Conclusion**

The Commission has been at the forefront of efforts to safeguard children's information online and to educate consumers about the risks involved in social networking. The agency is committed to continuing this important work. The FTC also is committed to working with this Subcommittee to provide greater security and privacy for American consumers.

MR. WHITFIELD. Thank you, Commissioner Harbour, and at this time, Mr. Ruiz, you are recognized for a 5-minute opening statement.

MR. RUIZ. Thank you. Good afternoon, Chairman Whitfield, Ranking Member Stupak, and other distinguished members of the subcommittee.

On behalf of the Federal Communications Commission, I would like to thank you for the opportunity to speak regarding the role of ISPs and social networking sites in the context of much needed efforts to protect the Nation's children from online exploitation and abuse. The

---

Civ. No. CV-04-1048 RJK (Ex) (C.D. Cal. Feb. 17, 2004) (civil penalty of \$75,000). Neither of these cases involved social networking sites.

<sup>16</sup> The COPPA Rule also empowers parents to protect their children under 13 even after consenting to a website operator's collecting information from them. If and when parents ask, site operators must provide them with the means to review the personal information that has been collected from their children. A site also must give parents the opportunity to prevent further collection or use of that information, as well as the chance to delete the information.

Commission shares the concern of Congress that children be protected from exploitation and abuse on the Internet. Given the importance of this issue and its implications for the safety and well-being of American families, the Commission is committed to working with Congress to do everything we can under the authority we are given.

As this subcommittee and Congress consider draft legislation to address the sexual exploitation of children over the Internet, we welcome your guidance on the Commission's role going forward. Should Congress choose to take action in this area, the Commission stands ready to implement any new mandates aggressively.

The Commission historically has had an important role in protecting children's interests and has implemented several programs intended to help protect children from exposure to inappropriate content over communications networks regulated by the Commission. For example, current Federal law restricts the broadcast of obscene, indecent, and profane programming. The Commission has implemented this law by adopting regulations which prohibit the broadcast of indecent material between the hours of 6 a.m. and 10 p.m., which are those hours of the day when children are most likely to be watching or tuning in.

In addition, the Commission has promulgated regulations prohibiting the broadcast of obscene material at any time, and Section 1464 of Title 18 prohibits the transmission of obscene content through any type of radio communications. The Federal Communications Commission has imposed substantial penalties where violations have been established. Indeed, Congress just recently amended the Communications Act to increase tenfold the forfeiture penalty for carrying indecent, obscene, or profane material. We believe that this should reduce the likelihood that some broadcasters might consider the forfeiture penalty for indecent programming an acceptable cost of doing business and will thus improve the effectiveness of our enforcement efforts in this area.

The Commission has also taken a variety of actions designed to help protect children from inappropriate content. Specifically, the Commission provides mechanisms to allow parents to restrict children's access to television programming by requiring that TV sets be equipped with V-chip technology. As you may know, V-chips allow the display of television program ratings which are derived from a voluntary system developed by the industry.

The Commission also provides a means to allow parents to block children's access to inappropriate content available over the telephone. Under the Commission's rules, local exchange carriers that are involved in transmitting and billing interstate pay per call and other information services, often referred to as 900 numbers, must offer an option to block access to such services.

And lastly, pursuant to Section 640 of the Communications Act, the Commission has adopted rules that require a cable operator upon subscriber request to fully scramble or block the audio and video portions of programming services not subscribed to by a household.

Unlike other entities, ISPs are subjected to limited regulations under the Communications Act. Nevertheless, in specific instances where the Commission does have authority, we have implemented programs governing the transmission of certain content by ISPs. For example, in 2005 in response to the request of Federal law enforcement agencies, the Commission ensured that the requirements of the Communications Assistant for Law Enforcement Act, or CALEA, extend to broadband Internet access services and voice over Internet protocol services, or VOIP services.

We have also implemented a program designed to help protect children who use the Internet in schools and libraries from accessing inappropriate content. In 1996 the Commission established the schools and libraries universal service support mechanism, commonly known as the e-rate program. In the year 2000 Congress adopted the Children's Internet Protection Act which provides that schools and libraries that have computers with Internet access must certify that they have in place certain Internet safety policies and technology protection measures in order to be eligible to receive support under the E-Rate program. The Commission established a corresponding regulation whereby in order to receive E-Rate funding, school and library authorities must certify that they are enforcing a policy of Internet safety that includes measures to block or filter Internet access to visual depictions that are, one, obscene, two, child pornography, or three, harmful to minors.

As Congress considers legislation in this area, it is important to keep in mind how any new legislative provisions might interact with the Communications Act's existing framework, in particular, which Section 503(B) of the Communications Act authorizes the Commission to impose forfeitures for violations of the Act as well as the Commission's rules and orders. Those who do not hold a license, permit, certificate, or other Commission authorization, as many ISPs do not, currently may not be fined by the Commission in the first instance. Rather, the Commission is first required to issue such entities a citation and then may only impose a forfeiture in the event that they again engage in the cited conduct.

In conclusion, I wish to reiterate the Commission's interest in taking action as appropriately directed by Congress in this important area. As I noted at the outset, the Commission stands ready to implement any new mandates aggressively.

Thank you again for the opportunity to testify before you today, and I would be pleased to respond to any questions you may have.  
[The prepared statement of Diego Ruiz follows:]



PREPARED STATEMENT OF DIEGO RUIZ, DEPUTY CHIEF, OFFICE OF STRATEGIC PLANNING  
AND POLICY ANALYSIS, FEDERAL COMMUNICATION COMMISSION

Good afternoon, Chairman Whitfield, Ranking Member Stupak and distinguished Members of the Subcommittee. On behalf of the Federal Communications Commission, I would like to thank you for the opportunity to speak regarding the role of Internet Service Providers (ISPs) and social networking sites in the context of the much needed efforts to protect the Nation's children from online exploitation and abuse.

The Commission shares the concern of Congress that children be protected from inappropriate content on the Internet. Given the importance of this issue and its implications for the safety and well-being of American families, the Commission is committed to working with Congress to do whatever is possible under the authority we are given. As this Subcommittee and Congress consider draft legislation to address the sexual exploitation of children over the Internet, we welcome your guidance on the role the Commission should have going forward. Should Congress choose to take action in this area, the Commission stands ready to implement any new mandates aggressively.

The Commission historically has had an important role in protecting children's interests and has implemented several programs intended to help protect children from accessing inappropriate content over communications networks regulated by the Commission. For example, current federal law restricts the broadcast of obscene, indecent, and profane programming. The Commission has implemented this law by adopting regulations which prohibit the broadcast of indecent material between 6:00 am and 10:00 pm, those hours of the day when children are most likely to be watching. Similarly, the Commission has also made it clear that profane language is prohibited from being broadcast during those same hours. In addition, the Commission has promulgated regulations prohibiting the broadcast of obscene material at any time.

The Commission has imposed substantial penalties where violations are established. Indeed, Congress just recently amended the Communications Act to increase by ten-fold the forfeiture penalty for carrying indecent, obscene or profane material. This should reduce the likelihood that some broadcasters will consider the forfeiture penalty for indecent programming an acceptable cost of doing business and will thus improve the effectiveness of our enforcement efforts in this area.

In the Communications Act, Congress has also prohibited cable systems from carrying obscene programming. And, a separate federal law similarly prohibits the distribution of obscene material via cable television. Finally, federal criminal law also clearly proscribes the distribution of obscenity and child pornography over the Internet though these statutes are enforced by the Department of Justice rather than the Commission.

The Commission has also taken a variety of actions designed to prevent children from accessing inappropriate content. Specifically:

- The Commission provides mechanisms to allow parents to restrict children's access to television programming by requiring that TV sets be equipped with V-chip technology. V-chips allow the display of television program ratings. The ratings system, which the FCC determined in 1998 met statutory requirements, relies on a voluntary system developed by the industry.
- The Commission provides a means to allow parents to block children's access to inappropriate content available over the telephone. Under the Commission's rules, local exchange carriers that are involved in transmitting and billing interstate pay-per-call and other information services, often

referred to as “900 numbers” must offer an option to block access to such services.

- Pursuant to section 640 of the Communications Act, the Commission has adopted rules that require a cable operator, upon subscriber request, to fully scramble or block the audio and video portions of programming services not subscribed to by a household.
- The Commission also administers provisions of the Children’s Television Act that require television broadcasters to provide programming designed to serve the educational and informational needs of children and limits the amount of advertising that such programming can contain.

Unlike other entities, ISPs are subject to limited regulation under the Communications Act. Nevertheless, where the Commission has authority, we have implemented programs governing the transmission of content by ISPs. For example, in 2005, in response to the request of a group of federal law enforcement agencies, the Commission ensured that CALEA’s requirements extend to broadband Internet access services and Voice Over Internet Protocol services. And, just last month, the Commission adopted an order providing further clarity to carriers and other new technology service providers regarding the implementation of their law enforcement obligations. Significantly, the Commission’s actions in this area were recently affirmed by the United States Court of Appeals for the District of Columbia Circuit.

We have also implemented a program designed to help protect children who use the Internet in schools and libraries from accessing inappropriate content. In 1996, the

Commission established the schools and libraries Universal Service support mechanism, known as the E-Rate program. In 2000, Congress adopted the Children's Internet Protection Act (CIPA), which provides that schools and libraries that have computers with Internet access must certify that they have in place certain Internet safety policies and technology protection measures in order to be eligible to receive discounted Internet access, Internet services, and internal connection services as part of the E-Rate program.

The Commission established a corresponding regulation. Accordingly, in order to receive support for Internet access and internal connections services under the E-Rate program, school and library authorities must certify that they are enforcing a policy of Internet safety that includes measures to block or filter Internet access to "visual depictions" that are (1) "obscene;" (2) "child pornography;" or (3) "harmful to minors." The relevant authority with responsibility for administration of the eligible school or library must certify its compliance for the purpose of CIPA in order to receive USF support.

As Congress considers legislation in this area, it is important to keep in mind how any new legislative provisions would interact with the Communications Act's existing framework. In particular, while section 503(b) of the Communications Act authorizes the Commission to impose forfeitures for violations of the Act as well as the Commission's rules and orders, those who do not hold a license, permit, certificate, or other Commission authorization, such as many ISPs, currently may not be fined by the Commission in the first instance. Rather, the Commission is first required to issue such

entities a citation and then may only impose a forfeiture in the event that they again engage in the cited conduct.

In conclusion, I wish to reiterate the Commission's interest in taking action as appropriately directed by Congress in this important area. As I noted at the outset, the Commission stands ready to implement any new mandates aggressively. Thank you again for the opportunity to testify before you today. I would be pleased to respond to any questions you may have.

MR. WHITFIELD. Thank you, Mr. Ruiz.

And Attorney General Blumenthal, we are glad to have you here. You are recognized for 5 minutes.

MR. BLUMENTHAL. Thank you, Mr. Chairman, and thank you for having me today.

Thank you most importantly for focusing this committee's interests on this topic of paramount importance not only here in Washington but as every one of you knows in your own homes, in your States and your communities, and I am here not speaking on behalf of the attorneys general but I think what I have to say pretty much reflects the way we feel and there is a group of 20-plus--it is now 21, perhaps more attorneys general that have been in touch in continuing discussions with MySpace and some of the other social networking sites directly face to face, through correspondence, which we would be happy to provide you, and also in other contexts such as the recent conference that the National Center for Missing and Exploited Children; they had a very excellent conference here in Washington, and I would like my testimony if it may be to be part of the record here and just perhaps speak and summarize from my impressions of this day, and I know the committee has been through other days of testimony.

I think the committee can sort of feel that there is a disconnect here. There is a disconnect between what you just heard from this table, the witnesses who have implied that everything is under control, everything is fine, everything is in place, and that which you heard from my colleague, and he is a colleague because I have worked with Detective Dannahey in Connecticut on some of these cases about the horrible, the horrific cases of sexual assault.

We are not talking about offensive images, about pornography. We can differ on what is pornography and what is sexually explicit and what is offensive but we are talking about sexual assaults on 12- and 13-year-olds, and I can provide the committee with more documentation on these contacts and how they led to these sexual assaults. So that is the first disconnect.

The second is what you just heard about the Internet sex offender registry. There is ongoing an effort to establish a national Internet registry of sex offenders. Connecticut has recently become a part of it. In my view, all the States eventually will be. It is the result of this Congress's initiative, the Jacob Wetterly Act, which in essence caused all of the States eventually to form these Internet registries, and I might just add as a footnote here, that I defended the Internet registry before the United States Supreme Court. I argued the case and we won it, nine to zero, over challenges based on privacy, due process. The courts understand, they get it, that this information is vital to be disseminated and it is vital for the social networking sites to use it.

Let me make a third point, and this one really relates to the recommendations and the very strong feelings among the attorneys general group that more can be and must be done. Raising the age level, age verification central. Put aside all the complexities, and there are a lot of complexities to having 85 million people--it is probably up to 90 million now--able to talk to each other in real time and yet these social networking sites are telling you we just can't tell how old they are. But the most telling fact is, they are doing nothing, nothing in MySpace to verify age at all.

Let me make a couple of suggestions. If you raise the age level, verification of age becomes easier because you have driver's licenses, you have credit cards, so they go hand in hand. Second, there are sites that require parental consent right now. There are companies in the United Kingdom that require parental consent that then is checked through driver's licenses, other information, email addresses. This system may not be foolproof at this point but it can be at least instituted to provide some verification. I have made a number of other recommendations here. I would be happy to talk about them at greater length.

I want to emphasize two points in conclusion. First, parents always should be, always will be the first line of defense. I say that as the parent of four teenagers, and knowing how challenging these issues can be, and we have all been there. The committee members have very eloquently discussed their own experiences. But parents have a responsibility. MySpace can help them, must help them to do better. We want MySpace and the other social networking sites to do a better job voluntarily. We would much prefer to avoid government intrusion, regulation, intervention, and that is one reason why we haven't set a deadline, we haven't sued anyone. We want it to be voluntary.

But let me go back to what I regard as kind of the elephant in the room, which is Mr. Walden's point. These sites have huge financial stakes. They are adding 250,000 people every day. That is bigger than any city in the State of Connecticut. They are adding the State of Connecticut every week, and their revenues are from advertising and their revenues are huge. MySpace alone has 15 percent of all the ads on the Internet. It was bought by Fox, the news corporation, less than a year ago, for \$580 million. It is estimated to be worth multiples of that amount now, \$3 to \$6 billion, maybe more. So the deep pockets are there and more can be done.

Thank you.

[The prepared statement of Hon. Richard Blumenthal follows:]

PREPARED STATEMENT OF THE HON. RICHARD BLUMENTHAL, ATTORNEY GENERAL, STATE  
OF CONNECTICUT

I appreciate the opportunity to speak on the critically important topic of making the Internet safe for children with an emphasis on social networking sites and the role of the ISPs

The Internet represents an enormous advance in technology and communications, providing ever-increasing benefits and significant gains in productivity for workers. It can bridge human differences and bring together people all over the world. Social networking sites, in particular, can offer opportunities for people to share information and ideas and form friendships.

The Internet has a dark side, susceptible to use by sexual predators in preying on unsuspecting, innocent children. Social networking sites provide fertile ground for sexual predators to peruse personal profiles while searching for their victims. Law enforcement authorities like my office have received numerous complaints from parents about questionable material -- including pornography -- on social networking sites. Even more alarming are sexual assaults on young girls, twelve and thirteen years old, who pose as older teenagers and unknowingly meet predators through networks such as MySpace, with tragic results.

I have been leading a multi-state working group consisting of 21 state attorneys general seeking important changes in the MySpace.com websites to provide children with greater protection from sexual predators and inappropriate material. While we seek voluntary measures from these websites, time is critical. So far, MySpace has taken baby steps, when major strides are needed. If the social networking sites fail to take specific steps recommended by the state attorneys general, Congress should act.

To adequately protect children, Congress should immediately consider:

- encouraging the restriction of all adult social networking sites to individuals 16 years and older while limiting teen access to sexually explicit materials on these sites;
- providing incentives for social networking sites to employ effective age verification methods;



- requiring all social networking sites to establish clear operating standards and employ an effective security system to monitor compliance with those standards and to work with law enforcement if potential criminal activity is detected;
- funding parent and child education programs through local law enforcement agencies;

Late last year, my office first received complaints from parents about MySpace.com , a social networking site with more than 85 million users. As you know, the site is designed to allow people to create their own personalized web pages, including children who have used the site to communicate with friends.

In reality, this site now exposes young people to a perilous cyberenvironment with people posting sexually explicit materials and looking for sexual relationships. Children can view pornographic images, links to x-rated websites, "clubs" involving adults seeking sexual encounters and webcam sex for sale offers.

Numerous sexual assaults on children in Connecticut have been directly linked to MySpace.com. In each instance, the predator established contact with the children through their MySpace.com pages.

MySpace has been engaged in constructive discussions with my office and the National Association of Attorneys General working group which I and North Carolina Attorney General Roy Cooper have led. In response to my concerns, MySpace has provided free software that parents can install to block their children's access to the site and hired a new security director --- but more needs to be done.

The first critical step must be keeping adults separate from children on any social networking site. For MySpace and similar social networking sites, no child under the age of sixteen years should be allowed access. Any social networking sites designed for children must provide heightened protection against access by sexual predators.

Second, all social networking sites -- regardless of whether they are designed for adults or children -- should employ effective age verification methods to ensure that children are not exposed to pornography, sexual predators and other inappropriate material. Adult age verification is neither novel nor cutting edge for the Internet. Many website operators have created systems to verify the user's age and identification. Under current case law, Congress may be limited in its ability to require age separation on these social networking sites. Therefore, Congress should be creative in designing incentives -- and perhaps disincentives -- for websites that fail to meet these standards.

Third, all social networking sites should fully disclose their operating standards -- who is allowed to establish and use profiles, how is the public allowed access to the site, what types of information are allowed or prohibited and so forth. These standards should be clearly and conspicuously disclosed on the website with easy ability to download and print the operating standards. The websites must devote adequate resources to effectively enforce violations of

their operating standards. Finally, each site should have an easily accessible filtering software that allows parents to block access to particular websites.

Fourth, parent and child education on website safety is absolutely necessary. In Connecticut, I have worked with local police chiefs in conducting community outreach programs. These programs have been well-received by parents. We need to do more. Congress should consider providing competitive grants and technical assistance, such as a best practices policy on internet safety, to local police departments and other law enforcement agencies.

Parents will always be the first -- and last -- line of defense, and should realize that responsibility. But MySpace must help them.

I commend the committee on their interest in this important subject. I look forward to working with the committee on creative solutions to protecting children and adults from Internet dangers.

MR. WHITFIELD. Thank you, Attorney General Blumenthal, and you are exactly right. There is a lot of money involved, and I read that article also about the purchase price that was paid for MySpace.com, and I do agree with you and I think all of us do know that this Internet registry of sex offenders would provide tremendous help to law enforcement and all of us. Could you explain to us what the status of that is right now? You were involved in a lawsuit over that.

MR. BLUMENTHAL. The law was challenged, the Internet registry was challenged, but it was upheld by the United States Supreme Court some years ago and many States, like Connecticut, have Internet registries that set forth relevant details about the criminal offense, name, address. One fact that could be added and it has been suggested here is email address.

MR. WHITFIELD. Right, right.

MR. BLUMENTHAL. And that very possibly is a fact that should be considered, and there are some downsides. There will be some arguments against it but it would at least permit in an email age some greater perspective and information out there.

MR. WHITFIELD. Who were the plaintiffs in that case that challenged the legality?

MR. BLUMENTHAL. The Connecticut Civil Liberties Union. It was a John Doe but he was represented by the Connecticut Civil Liberties Union.

MR. WHITFIELD. And you argued the case before the Supreme Court?

MR. BLUMENTHAL. Yes.

MR. WHITFIELD. Mr. Ruiz, Detective Dannahey talked to us about teenagers' access to cellular phones and how that is really going to make it more difficult to monitor as they can move pornographic sites, transmit pornographic photos, and so forth. Have there been any discussions

within the FCC about that issue and the reporting of those transmissions at all?

MR. RUIZ. Congressman, are you talking specifically about cellular phones?

MR. WHITFIELD. Requiring cellular phone companies to report the transmission of the images.

MR. RUIZ. I know that there have been efforts undertaken by the cellular phone industry to create parental block mechanisms and safeguards built into the devices and the functionalities that they offer. In terms of--and we have encouraged that effort.

MR. WHITFIELD. Requiring it to be reported to NCMEC?

MR. RUIZ. Not to my knowledge, sir, but I would have to take that back and get back to you on that.

[The information follows:]



Federal Communications Commission  
Washington, D.C. 20554

August 30, 2006

The Honorable Ed Whitfield  
Chairman  
Subcommittee on Oversight & Investigations  
Committee on Energy and Commerce  
U.S. House of Representatives  
2125 Rayburn House Office Building  
Washington, D.C. 20515

Dear Chairman Whitfield:

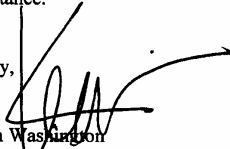
Please find enclosed a Declaratory Ruling released today by the Federal Communications Commission which is relevant to a question posed during the Oversight & Investigations Subcommittee hearing of June 28, 2006 entitled, "Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites."

During the hearing, you asked the Commission's witness, Mr. Diego Ruiz, if there has been any discussion within the Commission about requiring cellular carriers to report transmission of pornographic images over their networks to the National Center for Missing & Exploited Children. At that time, Mr. Ruiz stated he would provide additional post-hearing information for the record.

In the attached Declaratory Ruling, the Commission clarifies that section 222 of the Communications Act, which obligates carriers to protect the confidentiality of Customer Proprietary Network Information (CPNI), does not prevent a telecommunications carrier from complying with the obligation in 42 U.S.C. § 13032 to report violations of specific federal statutes relating to child pornography.

Please let me know if I can be of further assistance.

Sincerely,

  
S. Kevin Washington  
Director, Office of Legislative Affairs  
Federal Communications Commission

Enclosure

Before the  
Federal Communications Commission  
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of	)	
1996: Telecommunications Carriers' Use of	)	CC Docket No. 96-115
Customer Proprietary Network Information and	)	
Other Customer Information	)	

**DECLARATORY RULING**

**Adopted: August 30, 2006**

**Released: August 30, 2006**

By the Commission:

**I. INTRODUCTION**

1. By this Declaratory Ruling, we clarify that section 222 of the Communications Act of 1934, as amended (Communications Act), does not prevent a telecommunications carrier from complying with the obligation in 42 U.S.C. § 13032 to report violations of specific federal statutes relating to child pornography.

**II. BACKGROUND**

2. In section 222, Congress created a framework to govern telecommunications carriers' use of information obtained by virtue of providing a telecommunications service.<sup>1</sup> All telecommunications carriers, including wireless carriers, have a duty to protect the privacy of customer proprietary network information (CPNI).<sup>2</sup> Practically speaking, CPNI includes information such as the phone numbers called

<sup>1</sup> See 47 U.S.C. § 222. Section 222 was added to the Communications Act by the Telecommunications Act of 1996. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified at 47 U.S.C. §§ 151 *et seq.*). The Commission previously has described in detail the substance and history of carriers' duties relating to CPNI. See, e.g., *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*; *Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*; and *2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers*, CC Docket Nos. 96-115, 96-149, and 00-257, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rod 14860 (2002).

<sup>2</sup> CPNI is defined as “(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.” 47 U.S.C. § 222(h)(1). The Act defines subscriber list information as “any information – (A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and (B) that the carrier or

(continued....)

by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting. Section 222(c)(1) provides that, "[e]xcept as required by law," a telecommunications carrier that receives or obtains CPNI by virtue of providing a telecommunications service generally may only use, disclose or permit access to individually identifiable CPNI without customer approval in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.<sup>3</sup>

3. On our own motion, we address how telecommunications carriers' privacy duties under section 222 affect the requirement that suspected images of child pornography be reported to the CyberTipLine, operated by the National Center for Missing and Exploited Children (NCMEC), pursuant to 42 U.S.C. § 13032.<sup>4</sup> Specifically, 42 U.S.C. § 13032 requires providers of an "electronic communication service or remote computing service" to report apparent violations of certain federal statutes involving child pornography to the CyberTipLine operated by NCMEC, after which NCMEC in turn is required to forward that report to a law enforcement agency or agencies designated by the Attorney General.<sup>5</sup> "A provider of electronic communication services or remote computing services . . . who knowingly and willfully fails to make" such a report shall be fined up to \$50,000 for an initial failure to make such a report and up to \$100,000 for subsequent failures to make such reports.<sup>6</sup>

4. Congress has charged NCMEC with responsibility as a national resource center and clearinghouse for information regarding missing and exploited children.<sup>7</sup> NCMEC works in partnership with the Department of Justice, the Federal Bureau of Investigation and other state, federal, and international law enforcement authorities.<sup>8</sup> As part of its duties, NCMEC operates the CyberTipLine, which NCMEC describes as "an online reporting mechanism for child exploitation that is available to the public."<sup>9</sup>

### III. DISCUSSION

5. In this Declaratory Ruling, on our own motion, we find that the "except as required by law" exception contained in section 222(c)(1) of the Communications Act applies to any report required

(...continued from previous page)

an affiliate has published, caused to be published, or accepted for publication in any directory format." 47 U.S.C. § 222(h)(3).

<sup>3</sup> 47 U.S.C. § 222(c)(1). Section 222 also contains certain exceptions to this general restriction that are not germane to the issues addressed in this Declaratory Ruling. *See, e.g.*, 47 U.S.C. §§ 222(d) and (f).

<sup>4</sup> NCMEC has requested guidance on this and other related issues involving wireless services. *See Letter from Ernie Allen, President & CEO, NCMEC, to Kevin Martin, Chairman, FCC (Mar. 15, 2006) (NCMEC Letter).*

<sup>5</sup> 42 U.S.C. § 13032(b)(1); *see also* 28 C.F.R. §§ 81.11 to 81.13. The reporting obligation described in the text above specifically applies to whomever, "while engaged in providing an electronic communication service or a remote computing service to the public, through a facility or means of interstate or foreign commerce, obtains knowledge of facts or circumstances from which a violation of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 of Title 18, involving child pornography (as defined in section 2256 of that title), or a violation of section 1466A of that title, is apparent." 42 U.S.C. § 13032(b)(1). The statute does not require providers of an electronic communication service or a remote computing service to "engage in the monitoring of any user, subscriber, or customer of that provider, or the content of any communication of any such person." 42 U.S.C. § 13032(e).

<sup>6</sup> 42 U.S.C. § 13032(b)(4).

<sup>7</sup> 42 U.S.C. § 5771(5).

<sup>8</sup> *See id.*

<sup>9</sup> *See NCMEC Letter at 1.*

to be made by a telecommunications carrier to NCMEC pursuant to 42 U.S.C. § 13032.<sup>10</sup> Therefore, a telecommunications carrier does not violate section 222 to the extent it is compelled by 42 U.S.C. § 13032 to disclose CPNI in making such a report. Of course, this exception to section 222 only applies to the extent disclosure of CPNI is "required" and therefore would not cover voluntary disclosures.<sup>11</sup>

6. There is no need for us to analyze any particular providers or services to reach this result. The overlap between the two statutes – 47 U.S.C. § 222 and 42 U.S.C. § 13032 – only arises when a provider of electronic communication services or remote computing services<sup>12</sup> is a telecommunications carrier and is compelled to disclose CPNI. That is, to the extent an entity is not covered by the scope of 42 U.S.C. § 13032 as a provider of electronic communication services or remote computing services, it is not "required by law" to report instances of child pornography to the CyberTipLine by that statute. Similarly, if a provider compelled to make such a report is not a telecommunications carrier or the reporting obligation of 42 U.S.C. § 13032 does not require the disclosure of CPNI, section 222 does not restrict the provider's ability to report to the CyberTipLine. Thus, there is no circumstance in which making a report violates section 222.

#### IV. ORDERING CLAUSE

7. Accordingly, IT IS ORDERED pursuant to Sections 4(i) and 222 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 222 and sections 1.2 of the Commission's rules, 47 C.F.R. § 1.2, that this Declaratory Ruling IS ADOPTED effective immediately.

#### FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch  
Secretary

<sup>10</sup> 47 C.F.R. § 1.2 ("The Commission may, in accordance with section 5(d) of the Administrative Procedure Act, on motion or on its own motion issue a declaratory ruling terminating a controversy or removing uncertainty.").

<sup>11</sup> The "except as required by law" exception of 222(c)(1) is triggered only to the extent CPNI is required to be disclosed pursuant to 42 U.S.C. § 13032 or other legal requirement. 47 U.S.C. § 222(c)(1); 42 U.S.C. § 13032(d) (providing that a report to the CyberTipLine required by 42 U.S.C. § 13032(b)(1) "may include additional information or material developed by an electronic communication service or remote computing service, except that the Federal Government may not require the production of such information or material in that report").

<sup>12</sup> Section 13032(a) provides that "the term 'electronic communication service' has the meaning given the term in section 2510 of Title 18" and "'remote computing service' has the meaning given the term in section 2711 of Title 18." 42 U.S.C. § 13032(a). Thus, the term "'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications," 18 U.S.C. § 2510(15), and the term "'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system," 18 U.S.C. § 2711(2).

MR. WHITFIELD. If you would just reply to us and supplement the record on that point, I would appreciate that very much. Commissioner Harbour, you talked about the OnGuardOnline, and I would ask you,

how is that different from the advisories that you issue on the FTC's website?

MS. HARBOUR. Well, OnGuardOnline actually is on the website, but it is a multimedia website that deals with social networking; it deals with spyware adware; it deals with identity theft; it deals with spam. So for instance, regarding today's hearing on social networking, we have a site that talks about social networking specifically and in fact we have two pamphlets which I referenced in my testimony that target parents and one that targets teens, giving them advice about--

MR. WHITFIELD. And how do you market those or how do you get them out to the parents and the teenagers?

MS. HARBOUR. Seven of these social networking sites have links and we have commitments from 17 to link to our OnGuardOnline materials dealing with social networking. We also make our information available to law enforcement. I think that one of our crucial roles is getting the word out to our consumers, to our stakeholders, to parents, to Congress. Even when you break for the summer and you go back to your districts, it would be a wonderful thing to let your constituents know to educate them about some of the real perils on these social networking sites and perhaps encourage them to go to our site to look at our pamphlets. They were written specifically for parents in mind and also for teens and tweens.

MR. WHITFIELD. And what measures are in place to determine the effectiveness of what you are doing with OnGuardOnline?

MS. HARBOUR. Well, we know that we have had six to seven thousand hits each day in the past 2 months and we think that that increase in traffic has to do with our site being linked to some of the social networking sites and we will be vigilant in trying to get all of them to link to our materials.

MR. WHITFIELD. And let me ask you, the FTC, when you are talking about COPPA compliant, how do you determine if a social networking site is COPPA compliant?

MS. HARBOUR. Okay. What I referenced was COPPA, the Children's Online Privacy Protection Act, and it applies to sites directed at children under 13 or sites directed to general audience sites that have knowledge that they are collecting information from children under 13. So for instance, MySpace.com, for instance, if there were a child that they had knowledge was under the age of 13, that would implicate COPPA.

MR. WHITFIELD. Right.

MS. HARBOUR. And as they have indicated, they will screen out--

MR. WHITFIELD. And do you require these sites to register with the FTC?



MS. HARBOUR. These sites are not required to register. Basically COPPA requires the sites who collect information from children under the age of 13 to get verifiable parental consent to collect information from them.

MR. WHITFIELD. We are getting ready to have a series of votes on the floor so I am going to recognize Mr. Stupak to give him an opportunity to ask some questions.

MR. STUPAK. Thanks, Mr. Chairman, and I know we have seven votes coming up and I appreciate you all being here and helping us out. Should the sites be registered? Should these social networking sites be registered with the FTC?

MS. HARBOUR. When you say registered, Congressman, can you tell me what you mean by that?

MR. STUPAK. Well, give you notice where they are operating, the size of their use and things like this. I am trying to give you more information because quite frankly, until you mentioned your pamphlets, we had no idea on it, and if we don't know, we would probably be the ones who would read the pamphlets. The kids aren't reading these pamphlets. If it is not on the computer, it is not accessible, they are not going to read it. Even this so-called--this is MySpace terms and use agreement, it is eight pages long. I bet you there is not a kid in this country who probably read it. It is not cool enough. We don't read it. None of us read it even when we are supposed to read them, right? So why do you think a kid is going to read it? So that is what I am looking for, registries or something we could do through a registry that would help you.

MS. HARBOUR. What I think we really need to do is, we need to get the word out. We need to educate parents. We need to educate children about reducing the risks when they are online, and we are open to getting that word out. We have all of our material online.

MR. STUPAK. Well, along those lines then, Mr. Blumenthal, in your attorney generals' group, are you looking to target any of these sites? You mentioned the money they make off the advertising, of having to dedicate a certain amount or anything like that for advertising. I mean, I look at the Great Britain model and they had 18 percent of all the pornographic sites, if you will, down to four-tenths of one percent through that effective ad we saw earlier today. I don't see that happening in this country. Now, we saw some today which looked pretty effective, but in all honesty, I have never seen them, but I don't watch Fox either, so, I mean, I watch it at times but I have never seen it, and I should have asked the question when it was there. Have you guys come up with any kind of suggestions like that?

MR. BLUMENTHAL. We don't have suggestions for mandating spending of amounts of money on advertising. We are not in a sense in the business of telling these companies how to run their business. We are in the business of enforcing the law. And I must say, I am very gratified to hear that the FTC is investigating these sites for potential deceptive--and we are talking about basic deceptive and misleading practices under COPPA and that is a very important piece of news for me and I am delighted to learn it. But what we would like to do is see these sites use some of their revenues to educate. We think that would be a natural for them. It would be in their own interests. But at the same time, take these steps such as raising the age level, doing better age verification that they clearly have the resources to do.

MR. STUPAK. Have you seen any suggestions of making it mandatory in schools, cyber security as a class that would be taught?

MR. BLUMENTHAL. I know you asked that question, I believe you asked it earlier.

MR. STUPAK. Correct.

MR. BLUMENTHAL. And I think that would be an excellent suggestion. I realize there is always resistance--

MR. STUPAK. Sure.

MR. BLUMENTHAL. --to any, whether it's the State or the Congress, telling local school boards what to do but certainly by way of strong suggestion, it would be something to try to achieve. I think the one advantage of registration, to come back to your question, is that it would give the Congress or the Federal government more leverage over the sites, and must as we now do and I sort of am reminded of the discussion I had earlier this morning on hedge funds and obviously we are going through the whole issue of registration there, it provides a means of policing and assuring self-policing, which is what all of us would like to see.

MR. STUPAK. You indicated that you had some reports there that we might be interested in, and Mr. Chairman, I would move we make them part of the record. We don't have to go into them but I just think to complete the record and some of the work you have done and I think it would be important to have it in there.

MR. WHITFIELD. Without objection.

MR. STUPAK. You know, one of the problems we have seen in these sites, these ISP sites, I think testimony has been about 1,300 of them but only like 215 have voluntarily registered with NCMEC, right, and so that is why the FTC or FCC could be of help in trying to get these things registered so we know who they are, where they are, what they are and how to get to them. Mr. Attorney General, you sat through these hearings today, and just let me ask you this question. Is there anything

that was said that you would like to clarify or elaborate on? I know you have been through all these panels today. Is there anything else you wanted to say, because we are running out of time here and I know your time is precious also.

MR. BLUMENTHAL. Well, I appreciate that offer. What I would like to do with the Chairman's permission is perhaps supplement the testimony that I provided with some of the material that I have referenced and other points that perhaps some of my colleagues would like to add as well because I must say, this has been a very collegial effort on the part of the attorneys general obviously across the country, Republican, Democrat, and we would welcome the opportunity to continue to work with the committee.

MR. WHITFIELD. Absolutely, and we welcome the information.

MR. STUPAK. Mr. Chairman, one more before I yield back. Mr. Ruiz, in your testimony you mentioned the FCC was recently upheld in extending CALEA's requirements to broadband Internet access services. You indicate that many ISPs do not currently hold a license, permit, certificate, or other Commission authorization, even though other providers such as telephone companies and cable operators are required to file registration forms at the FCC. Does the FCC currently have any legal authority to require ISPs to register?

MR. RUIZ. The legal authority under which we require some ISPs to register, and specifically that is facilities-based broadband ISPs, it is Section 706 of the 1996 Communications Act, and that language was basically encouraging the rollout of broadband services to Americans so it is language first of all that is specific to facilities-based broadband ISP so it wouldn't cover--

MR. STUPAK. It wouldn't cover them?

MR. RUIZ. --dialup and it wouldn't cover any that are not facilities-based, and it really went to the issue of the rollout of the service as opposed to the specific issue of how that service is used, what content is transmitted over it, what kind of images--

MR. STUPAK. Does the FCC have the authority--we talked a lot about national standards or trying to move towards some national standards. The last panel mentioned it. Do you have any authority to convene all the ISPs to make them--but to reach an agreement on a common format for reporting to the NCMEC, to the National Center?

MR. RUIZ. Let me try to answer that, Congressman. To the extent we may have authority, it would be ancillary authority pursuant to our authority under Title 1 of the--

MR. STUPAK. But you could use your bully pulpit, couldn't you, and bring them together or maybe with the FTC too and--I am trying to find a way to move this--I think what we saw last panel, MySpace and all them,

they are trying to do the right things but I think these hearings we have been having have been pushing them but I want to keep the pressure on so we come up with some national standards, and I think they are all intending to and I think their heart is in the right place but once in a while we all need a shove. I am trying to get you guys to shove them.

MR. RUIZ. I understand, Congressman.

MR. STUPAK. With that, Mr. Chairman, I yield back. We have about 5 minutes left. I want to thank the witnesses. We read their testimony and it has been some interesting hearing, to say the least.

MR. WHITFIELD. We have had an interesting series of hearings and of course, we recognize there are many issues out there but one of the keys is what you pointed to, Attorney General Blumenthal. That is being able to really document and verify the ages of people who have access to these sites, and the suggestions about driver's licenses and parental consent were great suggestions and that is what is being done in Great Britain but we do thank all of you for your efforts in this area. We look forward to your continued leadership in this committee. I know the Chairman, Joe Barton, made the comment that he intends to come forward with some legislation to try to address this very complex issue. So we may be calling upon all of you for additional help, and without objection, I am going to move into the record the entire document binder, all the opening statements and certainly the material that you brought, Mr. Blumenthal, and thank you all again for being with us, and this hearing is adjourned, dismissed, over.

[The Information follows:]

Plaintiffs,

y.

**Defendants.**

IN THE DISTRICT COURT OF

TRAVIS COUNTY, TEXAS

261 JUDICIAL DISTRICT

**PLAINTIFFS' ORIGINAL PETITION**

Plaintiffs Jane Doe and Julie Doe (collectively, "Plaintiffs") seeks damages against Defendants MySpace Incorporated and News Corporation for negligence, gross negligence, fraud, fraud by nondisclosure and negligent misrepresentation – Defendants MySpace Incorporated and News Corporation are jointly and severely liable. Plaintiffs also seek damages against Defendant Pete I. Solis for sexual assault and intentional infliction of emotional distress. Plaintiffs would respectfully show the Court as follows:

I.

**PARTIES**

1. Plaintiff, Jane Doe, is a Texas resident and resides in Travis County, Texas. She is the parent and legal guardian of Julie Doe.
2. Plaintiff, Julie Doe, is a Texas resident and resides in Travis County, Texas. She is a 14-year-old minor.
3. Defendant, MySpace Incorporated ("MySpace"), is a Delaware Corporation and a wholly-owned subsidiary of Defendant News Corporation. MySpace has substantial,

PLAINTIFFS' ORIGINAL PETITION

by dice Ann Marting



continuous and systematic business contacts in Texas, and has committed tortious acts within Texas. MySpace may be served with process at their principal business address – 1333 2<sup>nd</sup> Street, Santa Monica, California, 90401.

4. Defendant, News Corporation (“News Corp.”), is a Delaware Corporation. News Corp. has substantial, continuous and systematic business contacts in Texas, and has committed tortious acts within Texas. News Corp. may be served with process at their principal business address – 1211 Avenue of the Americas, New York, NY, 10036.

5. Defendant, Pete I. Solis (“Pete Solis”), is a Texas resident and currently resides at 160 Calderon, Buda, Texas 78610. He may be served with process at this address or wherever he may be found.

## II.

### JURISDICTION AND VENUE

6. Jurisdiction over this case is proper as all parties reside in Texas, conduct substantial, continuous and systematic business in Texas, and/or have committed tortious acts within Texas. Plaintiffs seek damages, exclusive of interest and costs, in excess of the minimum jurisdictional limits of this Court. Furthermore, jurisdiction is proper in Texas under the Texas Long-Arm Statute, Tex. Civ. Prac. & Rem. Code § 17.041 *et seq.*, because Defendants MySpace and News Corp. have committed tortious acts in Texas and acts that constitute doing business in Texas.

7. Venue is proper in Travis County, Texas, pursuant to TEX. CIV. PRAC. & REM. CODE § 15.002(a), as all or a substantial part of the acts or omissions giving rise to Plaintiffs' claims occurred in Travis County, Texas. Venue is further proper because this court has personal jurisdiction over Defendants. Defendants have committed tortious acts in Texas, and/or Defendants have committed acts that constitute doing business in Texas.

III.

DISCOVERY LEVEL

8. Plaintiffs intend to conduct Level 3 discovery pursuant to TEX. R. CIV. P. 190.3.

IV.

FACTS

An Overview of MySpace

9. MySpace.com ("Myspace") is a social networking internet website where children and adults of all ages are encouraged to sign up and socialize in cyberspace. Founded in July 2003 by Tom Anderson and Chris DeWolfe, MySpace quickly exploded in popularity and became an online force to be reckoned with. In less than two years, MySpace has amassed more than 80 million registered users worldwide, and is the world's third most-viewed website.

10. In an attempt to capitalize on this success, Tom Anderson and Chris DeWolfe sold MySpace and its parent company, Internix Media, Inc., to News Corp. for an estimated \$649 million. News Corp. is a worldwide media conglomerate with approximately \$55 billion in total assets and approximately \$24 billion per year in annual revenues.

11. To access the social network, one must create a MySpace account. In order to create a MySpace account, all one has to do is enter a name, email address, gender, country, and date of birth. None of this information has to be true. MySpace does not have any verification mechanism in place to authenticate a new user's information. MySpace represents that a user must be at least 14 years of age to join – of course, this is not subject to any form of authentication. Thus, MySpace does not have any verification mechanism to ensure its users are of the age they claim to be, effectively providing a complete blanket of anonymity.

12. Once signed up, each MySpace user is given his or her own personal webpage to create. MySpace users are prompted to post photographs and personal information on their webpage. Typically, a MySpace user's webpage is viewable by any other MySpace user. Further, any MySpace user can contact any other MySpace user through internal email and/or instant messaging on MySpace.

13. MySpace currently has more than 80 million registered users online. It is also estimated that MySpace has over thirty (30) billion page views per month.<sup>1</sup> Ross Levinsohn, Senior Vice President and General Manager of Fox Interactive Media (a wholly-owned subsidiary of News Corp.), says that not even the internet giant Google.com believes it can provide enough advertisements to fill all the pages that MySpace displays each day.<sup>2</sup>

14. The catalyst behind MySpace's amazing surge in popularity is their underage users demographic. According to MySpace, approximately 22 percent of MySpace

<sup>1</sup> Michael Arrington, *The 27.4 Billion Pound Gorilla*, TechCrunch, June 13, 2006, at <http://www.techcrunch.com/2006/06/13/MySpace-the-27-billion-pound-gorilla>.

<sup>2</sup> Saul Hansell, *For MySpace, Making Friends Was Easy. Big Profit Is Tougher.*, The New York Times, April 23, 2006.



visitors are minors, under the age of 18.<sup>3</sup> MySpace actively and passively markets itself to minors.

15. Rupert Murdoch, News Corp. Chairman and Chief Executive Officer, is well aware that MySpace's continued success is directly tied into the website's appeal among young people, and the advertising revenue MySpace can generate.<sup>4</sup> The News Corp. CEO is adamant that MySpace CEO Chris DeWolfe find a way to make much more money from MySpace.<sup>5</sup> MySpace is projected to generate around \$200 million dollars in revenue this year, and has the potential to generate much more revenue as MySpace's popularity with the young teenagers continues to grow.<sup>6</sup>

16. The News Corp. CEO is equally aware of the dangers MySpace poses to underage minors using MySpace. While attempting to expand MySpace's success and popularity with underage minors, he has been increasingly confronted by state Attorney Generals across the United States and the public at large about the dangers Myspace poses to its underage users. Yet, Myspace has made no real effort to meaningfully increase the safety and security of their most important asset – young underage Myspace users. Sadly, Mr. Murdoch's initial strategy "seems to be to do nothing to interfere with whatever alchemy has attracted so many young people to MySpace in the first place."<sup>7</sup>

<sup>3</sup> Julia Angwin and Brian Steinberg, *News Corp. Goal: Make MySpace Safer For Teens*, *The Wall Street Journal*, February 17, 2006.

<sup>4</sup> Saul Hansell, *For MySpace, Making Friends Was Easy. Big Profit is Tougher.*, *The New York Times*, April 23, 2006.

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

17. MySpace proudly represents to parents and the public at large that teenagers under the age of 14 are not allowed to join MySpace. MySpace represents that the website has protections in place so that MySpace users ages 14 and 15 cannot be contacted by adult MySpace users. MySpace has publicly represented that the website is safe for its young underage users and that MySpace is doing everything to ensure it has adequate security measures in place to protect its young underage users.<sup>8</sup>

18. Despite MySpace's claims that Myspace is safe for young underage users, the facts suggest otherwise.

#### **Adult Sexual Predators on MySpace**

19. In the past year, a disturbing number of incidents have occurred nationwide in which adult MySpace users contacted young underage MySpace users on MySpace. The adult MySpace users then arranged to meet the minors and, often, sexually assaulted them. The following is a brief, non-exhaustive list, of a few of the criminal incidents that have resulted from adult MySpace users contacting young underage MySpace users on MySpace:

- a. On December 29, 2005, John David Payne of Brenham, Texas, was arrested for soliciting sex from young underage MySpace users. Mr. Payne thought he was chatting with young underage MySpace users on MySpace but, in reality, they were actually undercover investigators. On or about May 10, 2006,

<sup>8</sup> Julia Angwin and Brian Steinberg, *News Corp. Goal: Make MySpace Safer For Teens*, The Wall Street Journal, February 17, 2006.

Mr. Payne was again arrested for soliciting sex on MySpace from young underage MySpace users.<sup>9</sup>

b. On March 2, 2006, Federal prosecutors charged Sonny Szeto, 22, of New York, for using MySpace to meet an 11-year-old girl.<sup>10</sup>

c. On March 2, 2006, Federal prosecutors charged Stephen Letavec, 39, of Pennsylvania, for using MySpace to meet a 14-year-old girl.<sup>11</sup>

d. On May 1, 2006, Aaron Whitney, 27, of Chaplin, Connecticut, was charged with sexually assaulting a 13-year-old girl he met on MySpace.<sup>12</sup>

e. On May 6, 2006, Jesse Cahn, 22, of Stevens Point, Wisconsin, was charged with six counts of sexually assaulting a 14-year-old girl he met on MySpace.<sup>13</sup>

f. On May 12, 2006, Juan Gomez, 34, of Mount Vernon, New York, was charged with the felony of attempted dissemination of indecent material to a minor. Mr. Gomez contacted a 14-year-old girl on MySpace and engaged her in sexually explicit conversations. He was arrested when he attempted to meet the 14-year-old girl.<sup>14</sup>

<sup>9</sup> John Mortiz, *Attorney General Wants Web MySpace to Protect Young Users*, Fort Worth Star-Telegram, May 23, 2006.

<sup>10</sup> *MySpace.com to Bolster Security Measures*, Reuters Limited, March 3, 2006.

<sup>11</sup> *Id.*

<sup>12</sup> *Chaplin Man Arrested; Allegedly Met Girl, 13, on MySpace.com*, Norwich Bulletin, May 2, 2006.

<sup>13</sup> News Channel 7, Wausau, Wisconsin, at <http://www.wsaw.com/home/headlines/2815471.html>.

<sup>14</sup> *Ex-Teacher's Aide Caught in Pedophile Sting Operation*, North Country Gazette, May 12, 2006.

g. On May 15, 2006, Matthew R. Gale, 26, of Macomb, Illinois, was charged with six counts of aggravated sexual abuse and four counts of criminal sexual assault of a 16-year-old girl he contacted on MySpace.<sup>15</sup>

h. On May 22, 2006, a cyber crimes sting set up by the Texas Attorney General's Office netted the arrests of three adult men attempting to solicit sex from young underage MySpace users on MySpace.<sup>16</sup>

i. On May 29, 2006, prosecutors in Cleveland, Ohio, charged two adult men, Albert Azolino, 21, and Timothy Norman, 33, with sexually assaulting a 14-year-old girl they contacted on MySpace.<sup>17</sup>

j. On or about June 6, 2006, John Wentworth, 27, of Morris, Illinois, was charged with indecent solicitation of a child, attempted criminal sexual assault and aggravated criminal sexual abuse when he attempted to meet and sexually assault a 14-year-old girl he contacted on MySpace.<sup>18</sup>

k. On or about June 7, 2006, three Connecticut adult men were charged with numerous counts of sexual assault and risk of injury to a child for incidents involving two underage MySpace users they met on MySpace. Both girls were under the age of 16.<sup>19</sup>

<sup>15</sup> Stacey Creasy, *Police Dig into Suspect's Past*, Daily Review Atlas, May 15, 2006.

<sup>16</sup> News Channel 11, Houston, Texas at [http://www.khou.com/news/local/stories/khou060522\\_ac\\_cybercrimessting.061c54.html](http://www.khou.com/news/local/stories/khou060522_ac_cybercrimessting.061c54.html).

<sup>17</sup> News Channel 3, Cleveland, Ohio at [http://www.wkyo.com/news/watercooler/watercooler\\_article.aspx?storyid=51044](http://www.wkyo.com/news/watercooler/watercooler_article.aspx?storyid=51044).

<sup>18</sup> Jo Ann Hustis, *Man Charged with Solicitation*, Morris Daily Herald, June 12, 2006.

<sup>19</sup> Tom Kasprzak, *3 Connecticut Males Charged in Net Sex Case Connected to Stonington Girls*, The Westerly Sun, June 7, 2006.

l. On or about June 10, 2006, Shaun Roethlisberger, 21, of Duluth, Minnesota, was charged with two counts of third-degree criminal sexual conduct for having sexual intercourse with a 14-year-old girl he met on MySpace.<sup>20</sup>

m. On or about June 12, 2006, Jay Coffield, 44, of Naperville, Illinois, was arrested for soliciting sex from a 14-year-old girl he met on MySpace.<sup>21</sup>

#### Attorney Generals' Responses

20. The above-listed incidents have sparked considerable media attention and concern from the public. As a result of these incidents, several state Attorney Generals opened investigations into MySpace's lax security policies. They all concluded that despite MySpace's express representations to the public, MySpace has no meaningful security measures or policies in place to protect young underage MySpace users.

21. On February 2, 2006, Connecticut Attorney Richard Blumenthal opened a formal investigation into MySpace. On March 20, 2006, Attorney General Blumenthal sent MySpace, through their attorneys, a formal letter requesting, among other things, that MySpace: (1) raise the minimum age for a MySpace user from 14 to 16; and (2) require MySpace users to log in and verify their age before viewing profiles. *See attached, Exhibit A*, fully incorporated herein by reference.

22. On March 24, 2006, Ohio Attorney General Jim Petro sent MySpace Chief Executive Officer Chris DeWolfe a formal letter detailing that Ohio children were in danger due to the lax operating policies of MySpace and, among other things, urged MySpace to: (1) increase the minimum user age from 14 to 16; (2) prohibit adult users from accessing the profiles of young underage MySpace users; and (3) require that all

<sup>20</sup> Mark Stodghill, *Sex Offender Arrested*, Duluth News Tribune, June 10, 2006.

<sup>21</sup> *Police Say Man Arranged Sex with Girl, 14, on MySpace.com*, Chicago Tribune, June 11, 2006.

new users enter a verifiable credit card number during the registration process. *See attached, Exhibit B*, fully incorporated herein by reference.

23. Additionally, in March 2006, representatives for Massachusetts Attorney General Tom Reilly met with MySpace representatives to discuss their concerns about MySpace. Attorney General Reilly's office concluded that although MySpace maintains that only members under the age of 18 can view the profiles of members aged 14 to 15 years-old, their investigation revealed that MySpace does not have any system in place to verify its members' ages. Thus, nothing is preventing adult Myspace users from contacting young underage Myspace users.

24. On or about May 2, 2006, Attorney General Reilly sent a formal letter to MySpace company officials demanding that MySpace increase its minimum user age from 14 to 18 and institute an age and identify verification system. *See attached, Exhibit C*, fully incorporated herein by reference.

25. On May 22, 2006, Texas Attorney General Greg Abbott sent MySpace CEO Chris DeWolfe a notice letter expressing similar concerns. In it, Attorney General Abbott informed MySpace that:

*"By not requiring bank account information or a credit card in order to access your services, you have no way of authenticating the identify or age of your users, thereby providing a blanket of anonymity to those who wish to engage in criminal activity on your website. Although I understand you currently use an age verification system, our investigators have found it uncomfortably easy in a relatively short period of time to locate many underage profiles on your MySpace. A system of identity/age verification via credit card or a verified email account would be a better system than the current methods used by your web MySpace."* (emphasis added)

*See attached, Exhibit D*, fully incorporated herein by reference.

#### MySpace's Response

26. In light of these numerous incidents, pressure from Attorney Generals around the United States, and a growing media interest, MySpace representatives went on the defensive and issued numerous public statements emphasizing the safety of MySpace for young underage MySpace users. In February 2006, MySpace representatives told CBS News that:

“There are a number of specific procedures and policies in place to ensure users of all ages have a safe and meaningful experience. These include limiting use of the website to users who are at least 14 years of age and *providing special protections to users who are under 16 so that their personal information cannot be accessed by persons they do not know.*”<sup>22</sup>

27. MySpace also expressly represents these policies in the “Terms and Conditions” section on MySpace. MySpace claims that it is “illegal” or “prohibited” to “solicit personal information from anyone under 18.” MySpace also has a section entitled “Tips for Parents” where they state “MySpace members must be 14 years of age or older.”

28. Notwithstanding MySpace’s express representations to the contrary, problems of young underage MySpace users being contacted and sexually assaulted by adult Myspace users continue to plague MySpace. In further attempts to appease the public, in late April 2004, MySpace CEO Chris DeWolfe unveiled and widely-publicized a three-prong strategy to address growing safety concerns. The strategy included:

- (1) Putting in security technology, such as tools that allow children aged 14-16 years-old to shield their personal information from strangers;
- (2) Increasing manpower to review photos and images uploaded by MySpace users; and

<sup>22</sup> *MySpace.com Responds to Web Risks*, CBS News, February 6, 2006 (emphasis added).

- (3) Hiring Hemanshu Nigam (a former Federal Prosecutor, and so-called "Safety Czar") to head-up MySpace security.<sup>23</sup>

29. Unfortunately, MySpace's widely-publicized security strategy was simply public showmanship and a veiled attempt to appease the growing public outcry over their security concerns. MySpace knew that these measures did nothing to meaningfully increase the safety of young underage MySpace users. Yet, MySpace advertised it to the public as a substantial increase in the security of MySpace for young underage MySpace users. Tragically, by failing to properly address these concerns and institute meaningful security measures for young underage Myspace users, 14-year-old Julie was sexually assaulted by an adult MySpace user who found her on MySpace.

**The Sexual Assault of 14-Year-Old Julie Doe**

30. In the summer of 2005, 14-year-old Julie created a profile on MySpace. At the time, Julie was only 13-years-old. Despite MySpace's supposed rule prohibiting anyone under 14-years-old from using MySpace, Julie was able to create a profile. Julie did not regularly begin using MySpace until approximately February 2006.

31. On April 6, 2006, 19-year-old Pete Solis, an adult MySpace user, initiated contact with 14-year-old Julie on MySpace. 14-year-old Julie responded to Pete Solis' communications and thus began a series of emails between the adult MySpace user and 14-year-old Julie.

32. Pete Solis told 14-year-old Julie that he was a high-school senior that played on the football team. This was a lie. 14-year-old Julie told him she was a 14-year-old freshman in high-school. Pete Solis then quickly solicited and received 14-year-old

<sup>23</sup> Jesse Hempel, *From MySpace to Safer Place?*, BusinessWeek, April 11, 2006.



Julie's cell phone number. Pete Solis and 14-year-old Julie had several conversations over the phone as Pete Solis attempted to gain 14-year-old Julie's trust. It worked.

33. On May 12, 2006, Pete Solis arranged to meet 14-year-old Julie after school. Later that day, Pete Solis sexually assaulted 14-year-old Julie.

34. On May 13, 2006, Jane Doe called the Austin Police Department to report the sexual assault of 14-year-old Julie.

35. A detective from the Child Abuse Investigations Unit of the Austin Police Department conducted an investigation. In a videotaped confession, the adult MySpace user admitted to initiating contact with 14-year-old Julie on MySpace, soliciting her personal information, gaining her trust, and then sexually assaulting her. Pete Solis was arrested by the Austin Police Department for Sexual Assault, a 2<sup>nd</sup> Degree Felony, and is presently awaiting indictment.

V.

**CAUSES OF ACTION**

36. Plaintiffs fully incorporate all the facts averred above herein. All conditions precedent have occurred or have been waived.

37. MySpace actively and passively encourages young underage age children to join MySpace, and then directs them to communicate and socialize with complete strangers.

38. It is undisputed that MySpace's recent surge in popularity is driven by the onslaught of young underage users joining and using MySpace. To that end, MySpace has a very strong financial incentive to ensure that MySpace's popularity with young underage children remains intact, and continues to increase. MySpace has no financial incentive to institute any meaningful security measures to increase the safety of young

underage MySpace users. In fact, MySpace's interest is to ensure that access to MySpace by young underage children remains effortless and unfettered.

39. Despite MySpace's knowledge of the increasing occurrences of sexual assaults on young underage MySpace users by adult MySpace users, and despite MySpace's express representations to the contrary, there are absolutely no meaningful protections or security measures to protect young underage users from being contacted by adult sexual predators on Myspace.

40. MySpace's numerous representations to the public of "extra precautions" and "special protections" in place that "ensure users of all ages have a safe and meaningful experience" are false and dishonest. Attorney Generals' Offices across the United States have made it abundantly clear to MySpace for months that they are not the "leader in internet security" that they proclaim to be.

41. Despite all the warnings, the numerous incidents of sexual assaults on young underage MySpace users by adult MySpace users, and their widely-publicized claims of safety to the public, MySpace has still not instituted any meaningful changes or additional security measures to effectively increase the safety of their young underage users.

#### COUNT I – NEGLIGENCE

42. Plaintiffs fully incorporate all the facts averred above herein. All conditions precedent have occurred or have been waived.

43. MySpace constructed a website that allows people of any age to join and indiscriminately communicate with each other. MySpace actively encourages young underage children and adults to join MySpace and socialize with complete strangers.

44. MySpace expressly and implicitly represented that their website was safe for young underage users, but MySpace had actual and constructive knowledge that they had no meaningful security measures or policies in place to effectively safeguard young underage MySpace users from being contacted by dangerous adult MySpace users.

45. Furthermore, MySpace had actual and constructive knowledge of numerous sexual assaults and attempted sexual assaults of young underage MySpace users by adult MySpace users who used MySpace to initiate contact with them and draw them out.

46. MySpace owed a legal duty to 14-year-old Julie to institute and enforce appropriate security measures and policies that would substantially decrease the likelihood of danger and harm that MySpace posed to her.

47. MySpace breached their duty by publicly touting the effectiveness of their security measures and policies they knew or should have known were utterly ineffective in deterring the likelihood of danger and harm to 14-year-old Julie. MySpace also breached their duty by failing to act to substantially decrease the likelihood of danger and harm to 14-year-old Julie upon gaining actual and constructive knowledge of the danger and harm.

48. MySpace's breach of their duty proximately caused the sexual assault of 14-year-old Julie. The physical, psychological and emotional trauma 14-year-old Julie endured is indescribable and permanent. MySpace is the proximate cause of 14-year-old Julie's injuries.

49. Plaintiffs seek actual and exemplary damages against MySpace and News Corp. for MySpace's negligence.

50. MySpace and News Corp. are jointly and severely liable for these damages.

**COUNT II – GROSS NEGLIGENCE**

51. Plaintiffs fully incorporate all the facts averred above herein. All conditions precedent have occurred or have been waived.

52. MySpace has knowingly and purposely placed corporate greed over the health and safety of young underage MySpace users.

53. MySpace's actions, along with their omissions to act, when viewed objectively from their own standpoint, during the timeframe discussed *supra*, involved an extreme degree of risk and callousness. Particularly in light of:

- (1) MySpace's actual knowledge, awareness, and conscious indifference of the extreme dangers MySpace posed to young underage MySpace users;
- (2) MySpace's actual knowledge, awareness, and conscious indifference that adult MySpace users were able to contact and were regularly contacting young underage MySpace users, obtaining their personal information, and sometimes sexually assaulting them;
- (3) MySpace's actual knowledge, awareness, and conscious indifference to the warnings given them by Attorney Generals' Offices around the United States;
- (4) MySpace's actual knowledge, awareness, and conscious indifference to the misrepresentations they made to Plaintiffs and the public at large regarding the safety and security of MySpace for young underage MySpace users; and
- (5) MySpace's actual knowledge, awareness, and conscious indifference to not institute even the most minimal and inexpensive of security measures

that would greatly increase the safety of young underage MySpace users from being contacted by, exploited, and potentially assaulted by adult MySpace members.

54. From MySpace's standpoint there was a likelihood of serious injury and harm to young underage MySpace users, particularly 14-year-old Julie, and there was more than just a remote possibility of injury. MySpace had actual knowledge of other incidents that occurred in nearly the exact same manner as the incidents complained of herein (sexual assaults of young underage MySpace members by adult MySpace members), and to the exact same class of persons (young underage MySpace users).

55. MySpace's actions, along with their omissions to act, demonstrate a conscious indifference and utter disregard for the rights, safety, and welfare of young underage MySpace users, particularly 14-year-old Julie.

56. Plaintiffs seek actual and exemplary damages against MySpace and News Corp. for MySpace's gross negligence.

57. MySpace and News Corp. are jointly and severely liable for these damages.

#### **COUNT III – FRAUD**

58. Plaintiffs fully incorporate all the facts averred above herein. All conditions precedent have occurred or have been waived.

59. MySpace made express and implied representations to Plaintiffs, both directly and indirectly. MySpace posted express representations on MySpace and made numerous material and false express and implied representations to the public that MySpace was safe for young underage MySpace users. These material and false representations were untrue, deceptive and misleading.

60. MySpace made these material and false representations knowing they were false and/or made them recklessly without knowledge of their truth and as a positive assertion of fact.

61. MySpace made these material and false representations with the intent that Plaintiffs rely upon them and with the expectation that Plaintiffs would act in reliance on them.

62. Plaintiffs knew of MySpace's material and false representations, Plaintiffs relied upon them, and Plaintiffs' reliance was justifiable.

63. MySpace's material and false representations were the direct and proximate cause of Plaintiffs' injuries.

64. Plaintiffs seek actual, direct, consequential and exemplary damages against MySpace and News Corp. for MySpace's fraudulent conduct.

65. MySpace and News Corp. are jointly and severely liable for these damages.

**COUNT IV – FRAUD BY NONDISCLOSURE**

66. Plaintiffs fully incorporate all the facts averred above herein. All conditions precedent have occurred or have been waived.

67. MySpace concealed from and/or failed to disclose material facts to Plaintiffs regarding the lack of security and protections of MySpace for young underage users.

68. MySpace had a duty to Plaintiffs to disclose these material facts since they knew their voluntary and/or partial disclosures regarding the alleged security and protections in place for young underage MySpace users was misleading, untrue, and created a false impression. MySpace knew Plaintiffs were ignorant of these material facts and Plaintiffs did not have an equal opportunity to discover them.

69. Despite MySpace's duty to disclose these material facts they deliberately remained silent. By deliberately remaining silent and failing to disclose these material facts, MySpace intended to induce Plaintiffs to take action and/or refrain from taking action.

70. Plaintiffs relied on MySpace's nondisclosures, without knowledge of the undisclosed material facts, and Plaintiffs were injured as a result.

71. Plaintiffs seek actual, direct, consequential and exemplary damages against MySpace and News Corp. for MySpace's fraudulent conduct.

72. MySpace and News Corp. are jointly and severely liable for these damages.

**COUNT V – NEGLIGENCE MISREPRESENTATION**

73. Plaintiffs fully incorporate all the facts averred above herein. All conditions precedent have occurred or have been waived.

74. MySpace made express and implied representations to Plaintiffs in the course of MySpace's business and/or during transactions in which MySpace had an interest. MySpace knew or should have known that Plaintiffs were members of the class of persons that would receive their false and material representations. These false and material representations included misstatements of material facts and were made in regard to the security and safety of MySpace for young underage MySpace users.

75. MySpace supplied this false information for the guidance of others and Plaintiffs in their business.

76. MySpace did not exercise reasonable care or competence in obtaining and/or communicating information regarding the safety and security of MySpace for young underage MySpace users.

77. Plaintiffs justifiably relied on MySpace's negligent misrepresentations and were thereby injured. MySpace's negligent misrepresentations were there proximate cause of Plaintiffs' injuries.

78. Plaintiffs seek actual and exemplary damages against MySpace and News Corp. for MySpace's negligent misrepresentations.

79. MySpace and News Corp. are jointly and severely liable for these damages.

#### COUNT VI – SEXUAL ASSAULT

80. Plaintiffs fully incorporate all the facts averred above herein. All conditions precedent have occurred or have been waived.

81. Pete Solis acted intentionally, knowingly and/or recklessly when he sexually assaulted 14-year-old Julie.

82. As a direct and foreseeable result of Pete Solis' conduct, 14-year-old Julie was physically, emotionally and psychologically traumatized. These damages are permanent.

83. Plaintiffs seek actual and exemplary damages against Pete Solis for sexual assault.

#### COUNT VII – INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

84. Plaintiffs fully incorporate all the facts averred above herein. All conditions precedent have occurred or have been waived.

85. Plaintiffs are seeking relief on behalf of 14-year-old Julie for Pete Solis' intentional infliction of emotional distress.

86. Pete Solis acted intentionally and/or recklessly when he sexually assaulted 14-year-old Julie. Pete Solis' actions were intend to cause or were substantially certain to cause extreme emotional distress to 14-year-old Julie. Alternatively, Pete Solis' knew or should have known that his actions created a high degree of risk of harm to 14-year-old



Julie and he deliberately proceeded to act in conscious indifference and disregard to 14-year-old Julie.

87. Pete Solis' actions and conduct were extreme and outrageous. The sexual assault of 14-year-old Julie was so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency and is utterly intolerable in a civilized society.

88. 14-year-old Julie suffered extreme emotional distress due to the sexual assault inflicted on her by Pete Solis. This emotional distress continues to be extreme and severe. Pete Solis' actions proximately caused 14-year-old Julie's extreme and severe emotional distress.

89. No alternative cause of action would provide a remedy for 14-year-old Julie's extreme and severe emotional distress.

90. Plaintiffs seek actual and exemplary damages against Pete Solis for his intentional infliction of emotional distress on 14-year-old Julie.

#### VI.

##### JURY DEMAND

91. Pursuant to TEX. R. CIV. P. 216, Plaintiffs respectfully demand a trial by jury of all issues so triable. The appropriate fee has been tendered.

#### VII.

##### PRAYER FOR RELIEF

92. Accordingly, Jane Doe, individually, seeks recovery for all medical and psychological counseling expenses that have been incurred and may be incurred in the future, on behalf of Julie Doe, while Julie Doe is a minor.

93. Jane Doe, as next of friend of Julie Doe, her minor daughter, seeks compensatory and exemplary damages for Julie Doe's pecuniary loss, mental anguish, psychological trauma, pain and suffering, and emotional distress, in the past and the future, as well as future medical and psychological counseling expenses.

94. WHEREFORE, Plaintiffs request that this Court enter judgment against the Defendants as follows:

- (a) Compensatory damages of no less than Thirty (30) Million Dollars, the exact amount to be determined at trial;
- (b) Exemplary Damages, the exact amount to be determined at trial;
- (c) Reasonable and necessary attorneys' fees, expenses and costs of suit as provided by law;
- (d) Pre- and post-judgment interest on all amounts awarded at the maximum interest rate provided by law; and
- (e) Any further relief in law and in equity to which Plaintiffs may be justly entitled.

DATED: June 19, 2006

March 20, 2008

Attorney Christine Van  
Horn & Hamer, LLP  
Century Square  
3300 Linneman Square NW  
Washington, D.C. 20007

Dear Mr. Van:

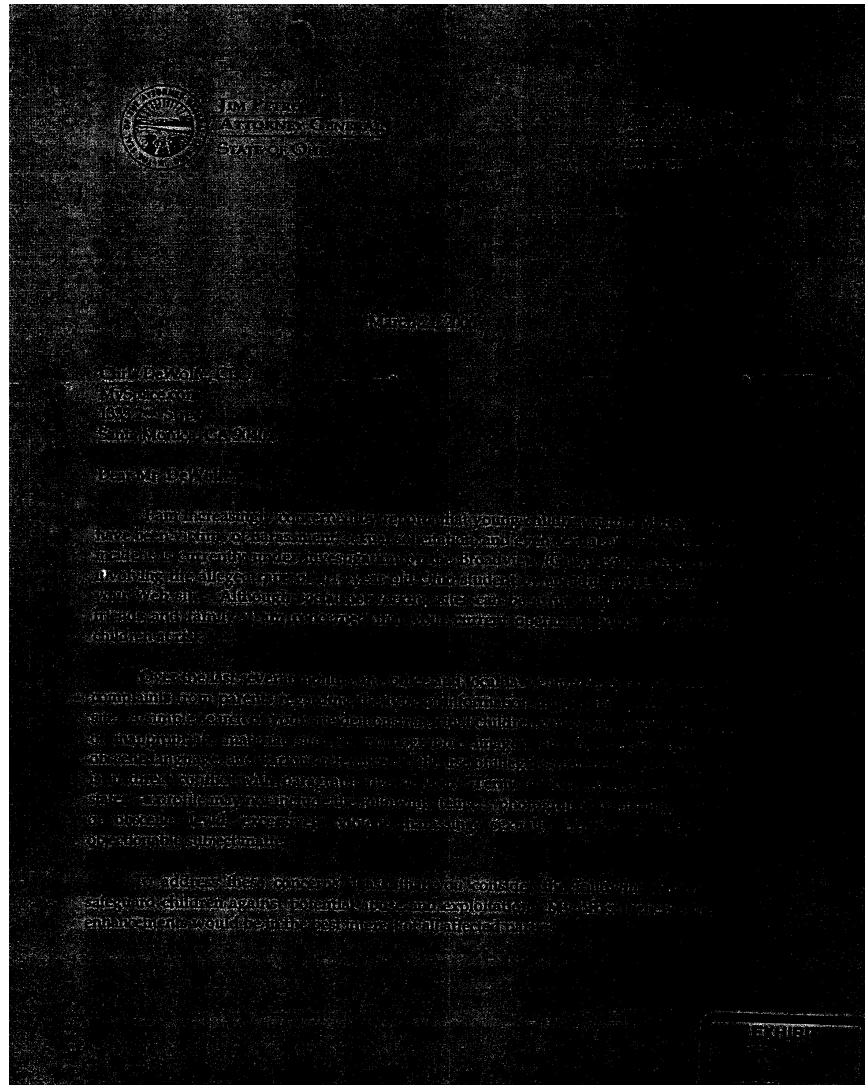
I have appreciated your responding to my letter of March 12, 2008, and I thank you for providing the opportunity to discuss your and your firm's views regarding Microsoft's Executive Office of Chief of Police and your continuing discussion.

The primary concern of my client, the Attorney General, is that the Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency. The Attorney General is concerned that the Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency. The Attorney General is concerned that the Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.

- 1. The Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.
- 2. The Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.
- 3. The Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.
- 4. The Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.
- 5. The Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.
- 6. The Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.
- 7. The Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.
- 8. The Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.
- 9. The Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.
- 10. The Microsoft Office of Chief of Police is not a law enforcement agency, but a law enforcement agency that is not a law enforcement agency.

EXHIBIT





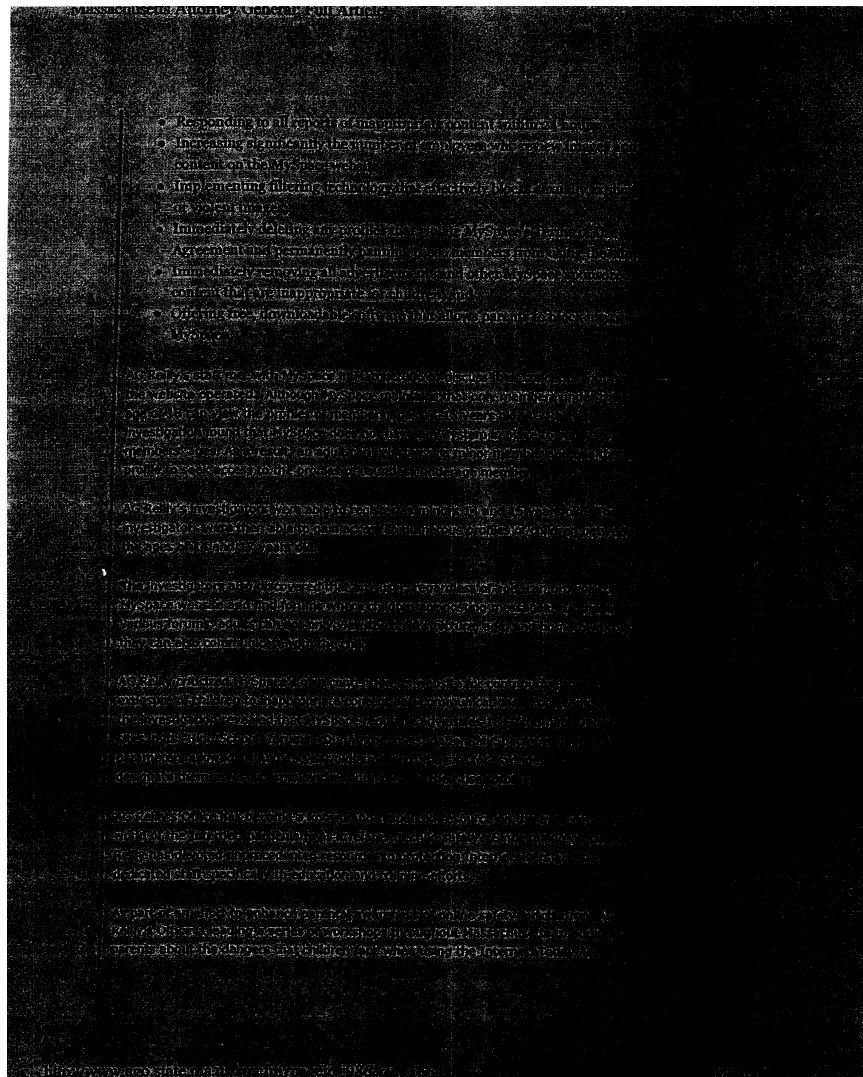




AG REPLY DEMANDS CHANGES TO  
MYSAPL.COM WEBSITE TO PROTECT TEENS  
FROM ONLINE PREDATORS

MAY 22 1986

**EXHIBIT**





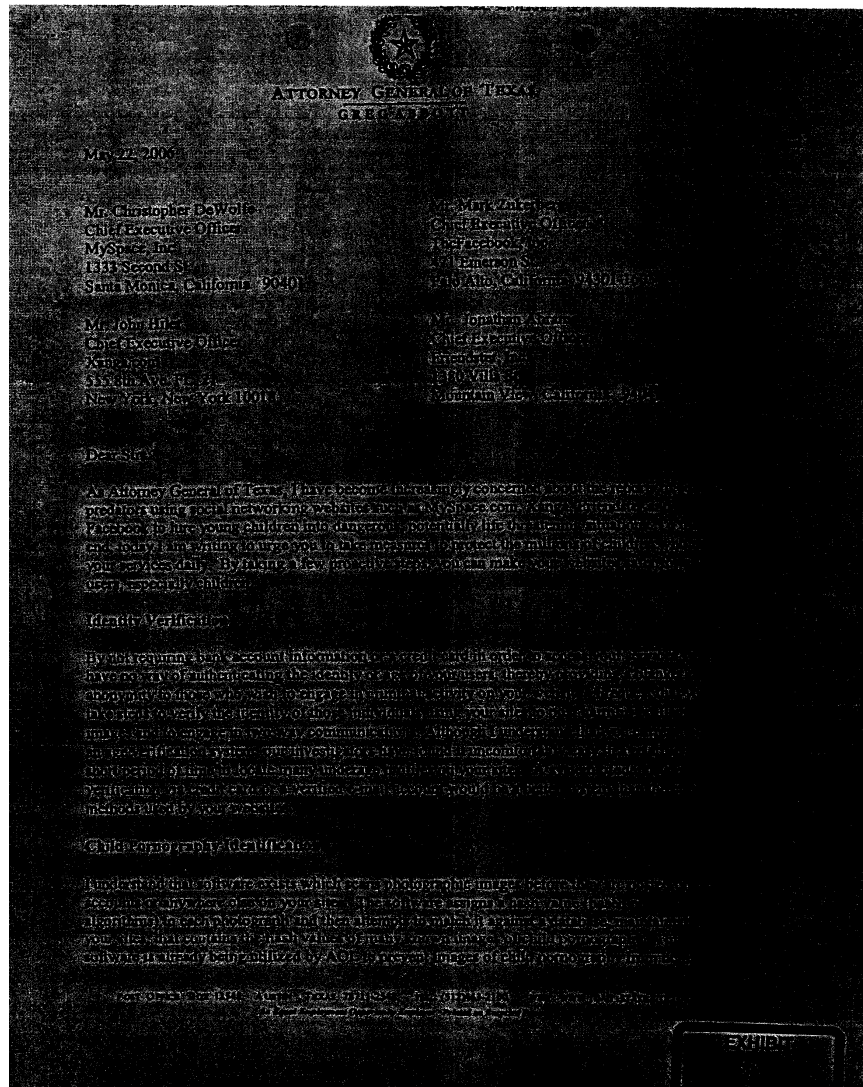
# Massachusetts Attorney General's Fall Article

Rally will conduct an Internet Safety program for parents in May to discuss warning signs of the potential dangers that exist when their children use the Internet. During AppleLink operation, AG Kelly charged that AppleLink is a deceptive and unfair business practice and that AppleLink is a deceptive and unfair business practice.

AG Kelly has also worked to make the Internet a safer consumer space by publishing a revised Consumer Guide to the Internet that now provides parents with ten key points that children's online activities should be safe. AG Kelly also has taken steps to make the Internet a safer consumer space by publishing a revised Consumer Guide to the Internet that now provides parents with ten key points that children's online activities should be safe.

Reference: [http://www.mass.gov/ag/](#)

AG Kelly has also worked to make the Internet a safer consumer space by publishing a revised Consumer Guide to the Internet that now provides parents with ten key points that children's online activities should be safe.



## References

[illegible]

OVER THE HILLS

[illegible]

Approved: \_\_\_\_\_  
 Attorney General

**Nelson, David**

---

**From:** Ertel, Elizabeth  
**Sent:** Friday, June 02, 2006 1:44 PM  
**To:** Nelson, David  
**Subject:** USA Today Article

Copyright 2006 Gannett Company, Inc.  
 All Rights Reserved  
 USA TODAY

June 1, 2006 Thursday  
 FINAL EDITION

**SECTION:** NEWS; Pg. 1A

**LENGTH:** 711 words

**HEADLINE:** U.S. asks **Internet** firms to savedata;  
 Could help fight terror, child porn

**BYLINE:** Jon Swartz and Kevin Johnson

**BODY:**

Top law enforcement officials have asked leading **Internet** companies to keep histories of the activities of Web users for up to two years to assist in criminal investigations of child pornography and terrorism, the Justice Department said Wednesday.

Attorney General Alberto Gonzales and FBI Director Robert Mueller outlined their request to executives from Google, Microsoft, AOL, Comcast, Verizon and others Friday in a private meeting at the Justice Department. The department has scheduled more discussions as early as Friday. Last week's meeting was first reported by CNET, an online news service.

The meetings reflect a new approach by law enforcement in anti-terrorism efforts. Previously, the Justice Department had invoked the need for data retention only to battle child pornography. Since the Sept. 11 attacks, **Internet** traffic has become increasingly critical to terrorism investigations, too.

Justice is not asking the companies to keep the content of e-mails, spokesman Brian Roehrkas said. It wants records such as lists of e-mail traffic and Web searches, he said.

Roehrkas said the government is required to seek proper legal authority, such as a subpoena, before obtaining the records. He said any change in the retention period would not alter that requirement. Law enforcement officials have seen investigations derailed "time and time again" because of a lack of data, Roehrkas said.

The government's request forces the companies to strike a balance between satisfying law enforcement demands and honoring the privacy of millions of customers.

"The issue for us is not whether we retain data, but we want to see it done right," says Dave McClure, president of the U.S. **Internet** Industry Association, which represents 150 companies, primarily **Internet** service providers. "Our concerns are who pays for it, what data is retained, and if it is retained legally without violating federal laws and subscriber agreements."

Lee Tien, a lawyer for the privacy advocacy group Electronic Frontier Foundation, said he was concerned.

"I think that the request raises some really, really major privacy problems," he said. The Justice Department is "asking ISPs (**Internet** service providers) to really become an arm of the government."

The request creates a logistical challenge: Most **Internet** providers store data such as Web searches for 30 to 90 days. Storing such information significantly longer is more expensive, McClure and others say.

"We strongly support Gonzales' interest in assuring that the **Internet** is safe for everyone," Phil Reitering, Microsoft's senior security strategist, said in a statement Wednesday that acknowledged the company's participation in the meeting at Justice. "But data retention is a complicated issue."

"We believe (data retention and preservation) proposals deserve careful review and must consider the legitimate interests of individual users, law enforcement agencies, and **Internet** companies," Google spokesman Steve Langdon said Wednesday.

Gonzales broached the issue of record retention in April during a speech at the National Center for Missing & Exploited Children in Alexandria, Va.

Gonzales, who has made fighting child exploitation a prominent part of the national law enforcement agenda, said the pursuit of child predators depends on the availability of evidence often in the hands of ISPs.

This isn't the first time Gonzales has gone to **Internet** companies with a request related to their records. In March, a federal judge ordered Google to hand over Web search records requested by Justice as part of its efforts to shield children from sexually explicit material online. Google balked at an earlier request, saying it would expose trade secrets. AOL, Yahoo and Microsoft cooperated with the government, but they said their assistance was limited and users' privacy was not violated.

Contributing: William M. Welch  
Retaining user records

\*What's kept now: An amendment to the 1986 Stored Communications Act permits the federal government to request that companies with **Internet** services retain records and other evidence -- lists of e-mail traffic and Web searches -- for 90 days.

\*What could change: The Justice Department wants records kept for up to two years to assist in terrorism and child-pornography investigations.

**Nelson, David**

---

**From:** Andrews, Kelli  
**Sent:** Monday, June 19, 2006 9:10 AM  
**To:** Nelson, David; Ertel, Elizabeth  
**Subject:** FW: Comcast

Examples from an ICAC officer on Comcast issues.

Kelli Andrews  
Majority Counsel  
Committee on Energy & Commerce  
Oversight & Investigations  
316 Ford House Office Building  
Washington, DC 20515

202/226-2424 (phone)  
202/226-2447 (fax)

---

**From:** Rob Jones [mailto:jones@helicon.net]  
**Sent:** Friday, June 16, 2006 1:16 AM  
**To:** Andrews, Kelli  
**Subject:** Comcast

Kelli,

The attachment labeled "Peer Cases" are IP addresses that I attempted to obtain subscriber and billing information on through Comcast. As you can see, the same address was requested on two separate occasion with different dates and times and they were still unable to recover any records. These cases involved unknown suspects in the Pittsburgh area distributing child pornography via peer to peer file sharing networks. Due to the inability to obtain customer records, the cases were unable to be prosecuted and the identities of the suspects will likely never be known.

The second case, with the attachment named "Reaney", was an undercover case where the suspect, Sean Reaney, admitted a desire to molest children. During our first chat session he spoke of this and sent me an email which enabled me to capture his IP address. As you can see, Comcast was unable to provide records on a three day old IP address. Fortunately, I chatted with Reaney again and he sent me another email which gave me his address which was traced back to his residence. If I hadn't met him online a second time, he may have never been apprehended.

Here is a news link to the story:

[http://www.pittsburghlive.com/x/pittsburghtrib/search/s\\_427206.html](http://www.pittsburghlive.com/x/pittsburghtrib/search/s_427206.html)

If you have any questions, please don't hesitate to contact me,

**Rob Jones**  
**Greensburg Police Department**  
**PSP Area III Computer Crime Task Force**  
**PA ICAC Task Force**

06/26/2006

**FBI MVHTCTF**  
**416 South Main Street**  
**Greensburg, Pa 15601**  
**724-834-3800**

06/26/2006

**Comcast****CONFIDENTIAL**

Comcast IP Services  
650 Centerton Road  
Moorestown, NJ 08057  
856.638.4022 Tel  
856.638. Fax

February 17, 2006

**VIA FACSIMILE**

Officer Robert Jones  
Greenburg Police Department  
416 South Main Street  
Greensburg, PA 15601  
Fax: 724-838-4304

Re: Court Order  
Case No.: 73 MISC 2006  
Our File #: 1061458 & 1061459

Dear Officer Jones:

The Court Order dated February 9, 2006 with respect to the above-referenced matter has been forwarded to me for a reply. The Court Order requests Comcast to produce certain subscriber account records pertaining to the following IP addresses: 24.3.96.53 and 67.171.85.245 on February 7, 2006 at 12:15 AM EST.

Based on the information provided pursuant to the Court Order, we are unable to find any information responsive to the request. Upon receipt of the Court Order we initiated our investigation. We discovered that the log files we use to make subscriber account identifications were either incomplete or contained an error associated with the registration of the cable modem or other device in question. Therefore, Comcast cannot identify the subscriber account associated with this request.

If I can be of further assistance, or if you have any questions regarding this matter, please feel free to call me at 856.638.4022.

Very Truly Yours,

*Kathleen Loughrin*  
Kathleen Loughrin  
Policy Abuse Legal Analyst



**Comcast**

**CONFIDENTIAL**

**VIA FACSIMILE**

Off. Rob Jones  
Greensburg Police Department  
416 South Main Street  
Greensburg, PA 15801  
Fax: (724) 838-4304

Comcast National IP Service  
650 Centerlon Road  
Moorestown, NJ 08057  
856.324-2128 Tel  
856.317-7318 Faxes

December 14, 2005

Re: Court Order  
Case No: 749MISC2005  
Our File #: 914184

Dear Mr. Jones:

The Court Order dated December 12, 2005 with respect to the above-referenced matter has been forwarded to me for a reply. The Court Order requests Comcast to produce certain subscriber account records pertaining to the following IP address: 68.81.205.233 on December 9, 2005 at 2:46 am and 3:15 am EST.

Based on the information provided pursuant to the Court Order, we are unable to find any information responsive to the request. Upon receipt of the Court Order we initiated our investigation. We discovered that the log files we use to make subscriber account identifications were either incomplete or contained an error associated with the registration of the cable modem or other device in question. Therefore, Comcast cannot identify the subscriber account associated with this request.

If I can be of further assistance, or if you have any questions regarding this matter, please feel free to call me at (856) 324-2125.

Very Truly Yours,

*Cris Coyle*

Cris Coyle  
Policy Abuse Legal Analyst

**Comcast****CONFIDENTIAL**

Comcast IP Services  
650 Criterion Road  
Moorestown, NJ 08057  
856.317.7272 Tel  
856.317.7197 Fax

March 1, 2006

**VIA FACSIMILE**

Officer Robert Jones  
Greensburg Police Department  
416 South Main Street  
Greensburg, PA 15601  
Fax: 724-838-4304

Re: Court Order  
Case No.: 98 MISC 2006  
Our File #: 1092291


Dear Officer Jones:

The Court Order dated February 22, 2006 with respect to the above-referenced matter has been forwarded to me for a reply. The Court Order requests Comcast to produce certain subscriber account records pertaining to the following IP address: 67.171.85.245 used at various times during January and February 2006.

Based on the information provided pursuant to the Court Order, we are unable to find any information responsive to the request. Upon receipt of the Court Order we initiated our investigation. We discovered that the log files we use to make subscriber account identifications were either incomplete or contained an error associated with the registration of the cable modem or other device in question. Therefore, Comcast cannot identify the subscriber account associated with this request.

If I can be of further assistance, or if you have any questions regarding this matter, please feel free to call me at 856.638.4022.

Very Truly Yours,



Kathleen Longhrin  
Policy Abuse Legal Analyst

## TRIBUNE-REVIEW

### Bucks County man charged in porn case

By Bob Stiles  
TRIBUNE-REVIEW  
Friday, February 24, 2006

A Bucks County man was charged Thursday with crimes related to child pornography, Greensburg police said.

Sean E. Reaney, 20, of 102 Sharp Lane, Feasterville, was arraigned yesterday before District Judge James Albert, of Greensburg, on 20 counts involving sexual abuse of children, unlawful contact with a minor, criminal use of a communication facility and corruption of minors.

In an arrest warrant affidavit, Greensburg Patrolman Robert Jones, a member of the Pennsylvania Internet Crimes Against Children Task Force, said that in December, he posed as a 14-year-old girl from the Greensburg area and entered an Internet chat room where he encountered a person who identified himself as "gothyboypa" and later as "Sean."

Sean related that he was 20, lived in the Philadelphia area and offered to show Jones videos of various sex acts and "assorted normal stuff" via their computer hookups, according to the affidavit. The movies relayed through the computers and a Web cam appeared to depict children, all less than 10 years old, engaged in various sex acts, Jones said.

Jones said he linked the involved computer communications and "Sean" to Reaney and his home address. Bucks County detectives then seized Reaney's computer system and other items from his bedroom.

Reaney admitted to detectives that he used the computer name of "gothyboypa," but denied having or sending child pornography, the court papers said.

Jones said he copied the movies he viewed via his and Reaney's computer hookup and sent them to the National Center for Missing and Exploited Children. The center confirmed that some of the videos contained "identified children" and were part of known collections of child pornography, the affidavit said.

Reaney, who surrendered to authorities while accompanied by his attorney and family, is free on \$50,000 unsecured bond. Court officials said that Reaney majors in computer science at an unspecified college and earns extra money by doing computer repairs.

Earlier this month, Greensburg police saw other child pornography videos being offered on the Internet and contacted authorities in Adams County, where the

suspects lived.

Liberty Township police then charged Ralph Douglas Tracy, 39, and Bryan Varner, 30, both of the township near Gettysburg, with numerous counts of crimes, including some related to child pornography.

*Bob Stiles can be reached at [bstiles@tribweb.com](mailto:bstiles@tribweb.com) or (724) 836-6622.*

Images and text copyright © 2006 by The Tribune-Review Publishing Co.  
Reproduction or reuse prohibited without written consent from [PittsburghLIVE.com](http://PittsburghLIVE.com)

**Nelson, David**

**From:** Robert.B.Parmiter@usdoj.gov  
**Sent:** Wednesday, May 17, 2006 1:14 PM  
**To:** Robert.B.Parmiter@usdoj.gov  
**Subject:** PREPARED REMARKS OF ATTORNEY GENERAL ALBERTO R. GONZALES AT THE PROJECT SAFE CHILDHOOD IMPLEMENTATION LAUNCH



ole0.bmp



ole1.bmp

FYI.

FOR IMMEDIATE RELEASE AG

WEDNESDAY, MAY 17, 2006 (202) 514-2007

WWW.USDOJ.GOV

TDD (202) 514-1888

PREPARED REMARKS OF ATTORNEY GENERAL ALBERTO R. GONZALES

AT THE PROJECT SAFE CHILDHOOD IMPLEMENTATION LAUNCH

WASHINGTON

Good morning. I am joined by FBI Director Robert Mueller; Assistant Secretary for Immigration and Customs Enforcement, Julie Myers; President of the National Center for Missing and Exploited Children, Ernie Allen; Deputy Director of the Secret Service, Mark Sullivan; Assistant Inspector in Charge of the United States Postal Inspection Service, Ray Smith; and Lieutenant Mike Harmony from the Bedford County Sheriff's Department and Joe Laramie from the Glendale, Missouri Police Department, two leaders of the Internet Crimes Against Children program.

This group is an indication of widespread cooperation throughout the law enforcement community. There won't be time for everyone to speak today, but I can assure you that each of these leaders represents a vital element of the program we are here to discuss today.

It has been estimated that, at any given time, 50,000 predators are on the Internet prowling for children. Just this morning, I visited the FBI's Innocent Images Unit in Maryland, where I observed some of the aggressive behavior and graphic language used by these online pedophiles as they solicit our children.

I've also seen depraved examples of child pornography, including the sexual abuse of children as young as infants. Words simply cannot describe how unsettling these images are.

It is not an exaggeration to say that we are in the midst of an epidemic of sexual abuse and exploitation of our children.

At the Department, we are working more of these disturbing cases than ever before - thanks to a dedicated team of investigators and prosecutors.

But we need to do more. Today, the Justice Department will begin to implement a new program to better protect our children from sexual abuse and exploitation through the Internet.

Project Safe Childhood will help law enforcement and community leaders develop a

coordinated strategy to prevent, investigate, and prosecute sexual predators, abusers, and pornographers who target our children. It begins not one moment too soon.

Law enforcement professionals at every level - and many partners who have joined me here today - understand the urgency for Project Safe Childhood.

Fighting alongside federal law enforcement officials are every day heroes at the State and local level, including our partners in the Department-funded, regional Internet Crimes Against Children Task Forces (ICACs). The Justice Department will be awarding more than \$14 million dollars to fund the ICACs this year - including, I am pleased to announce today, the formation of a new Task Force in southern Texas.

We also rely on our long-standing partner the National Center for Missing and Exploited Children, and other non-profit groups dedicated to keeping our children safe online such as i-Safe, Web Wise Kids, NetSmartz, and many more. The Office of Justice Programs will devote nearly five million dollars this year to Internet safety programs that help educate our children and their parents about the dangers of online predators.

These partners - and many others - will be vital to the success of this new initiative, and I am happy to have their support.

Here's how Project Safe Childhood works.

I've asked every United States Attorney to take the lead on implementing Project Safe Childhood with local partners in their communities. Within two weeks, every U.S. Attorney will review the guide we've published, designate a Project Safe Childhood Coordinator, and begin with three major steps to put this important program into action.

The first step is to build partnerships and capitalize on the experience of our existing partners. U.S. Attorneys will engage everyone with a stake in the future of our children. Together, they will inventory the unique nature of the challenge and the resources available in the community.

Second, these partners will work together as U.S. Attorneys develop a strategic plan for Project Safe Childhood in their area. I've asked U.S. Attorneys to develop these road maps for implementation within 90 days.

Lastly, we'll be ensuring accountability by requiring semi-annual progress reports. We want to know that Project Safe Childhood is having a measurable impact in terms of locking away criminals and identifying and rescuing child victims.

Project Safe Childhood will help make law enforcement more coordinated and better trained as they work to protect our children on the Internet. In addition, we need better legislation; both Houses of Congress have passed legislation addressing crimes against children and I urge Congress to complete this important work and send the President legislation for his signature in the near future. I know that these things will make a real difference in the lives of so many Americans.

I realize that child pornography and sexual enticement are not the only criminal activities that threaten our society. Obscenity debases men and women, fostering a culture in which these heinous crimes against our children become acceptable. That's why I formed the Obscenity Prosecution Task Force in the Criminal Division, which has worked together with their partners to investigate obscenity cases.

Project Safe Childhood will not detract from our efforts in this area; it will enhance our commitment to protect all Americans from these depraved crimes. As a father and a citizen, I care deeply about these issues. And as the chief law enforcement officer, I've made it a priority for the Justice Department to prosecute obscenity, child pornography, and sexual enticement cases.

President Bush has said that "anyone who takes the life or innocence of a child will be punished to the full extent of the law." He has given me the charge of protecting our children from these profound evils.

That is why we are launching Project Safe Childhood - to go after those criminals who would exploit the innocence and steal the dreams of our children.

**EMBARGOED FOR RELEASE**  
**12:01 a.m. Eastern, Tuesday, June 27, 2006**

**ONLINE INDUSTRY LEADERS ANNOUNCE NEW EFFORT TO USE  
ADVANCED TECHNOLOGIES TO COMBAT CHILD EXPLOITATION**

**AOL, Yahoo!, Microsoft, EarthLink, and United Online Announce Creation  
of Center for Child Protection Technologies at NCMEC**

**Center Will Establish Clearinghouse for Known Illegal Images,  
Offers Tools To Help Industry Disrupt Distribution of Known Images**

Washington, DC – June 27, 2006 – Five major online companies today announced that they are joining with the National Center for Missing and Exploited Children (NCMEC) to launch an aggressive new campaign against child exploitation on the Internet. AOL, Yahoo!, Microsoft, EarthLink and United Online will fund a new Center for Child Protection Technologies within NCMEC to develop and deploy technological solutions that disrupt the ability of predators to use the Internet to abuse children.

The Center will have four principal objectives:

- **Developing and Implementing Technology Solutions:** By identifying and developing existing and new technologies that can detect and disrupt the distribution of known images of child exploitation on the Internet.
- **Improving Knowledge Sharing Among Industry:** By establishing a centralized clearinghouse for known images of child pornography and other information that network operators can use to combat or block child pornography.
- **Improving Law Enforcement Tools:** By researching and developing tools for law enforcement to assist in the location and identification of predators and distributors of child pornography.
- **Research Perpetrators' Technologies to Enhance Industry Efforts:** By evaluating the specific and emerging technologies used by child predators to exploit children and conceal their activity.

The participating companies have committed \$1 million in combined initial funding to establish the Center. Beyond financial support, the coalition companies also agreed to offer the full backing of their collective experience, knowledge, and expertise in helping the Center address these issues.

CONFIDENTIAL DRAFT—Subject to participant comments

"Child predators take advantage of Internet technologies not only to help distribute images of child exploitation, but also to attempt to conceal their criminal behavior," said Ernie Allen president and CEO of NCMEC. "These leading companies have a wealth of expertise and technological tools that can help protect children and reduce the proliferation of sexually abusive images of children. Similar tools have been used to protect users from other Internet-related threats. Now they can also be applied to this fight against child pornographers."

The Center's initiatives would be structured to ensure that privacy interests of Internet users are appropriately balanced with its mission to interdict child pornography.

The participating coalition companies announced that an organizational conference would be held in July 2006 to draft the Center's charter and to evaluate a timeline for identification and deployment of technologies. The Center's goal is to establish the clearinghouse of known illegal images by the end of 2006.

"It may not be possible to eradicate all threats to children online, any more than it is possible to protect children from all threats in the physical world," said John Ryan, Chief Counsel of AOL. "However, by better leveraging 21<sup>st</sup> century technologies, we believe it is possible to increase the chance that child predators will be caught and provide a deterrent to those who would be tempted to exploit children on the Internet. The proposed Center would employ the best minds of the Internet industry to develop deterrent strategies and technologies."

"The unity of action behind this proposal is important because child safety is truly an industry issue," said Elizabeth Banker, Vice President and Associate General Counsel for Yahoo!. "This initiative is an expansion of Yahoo!'s long-term relationship with NCMEC and our industry peers, and we look forward to making real progress through the Center."

"Microsoft is steadfast in our commitment to combat all forms of child exploitation on the Internet," said Tim Cranton, Director of Internet Safety Enforcement Programs at Microsoft Corp. "Our partnership with NCMEC and other online industry leaders in this technology initiative is an essential next step in the effort to identify and implement technology solutions that can help protect children from Internet predators and inappropriate online material."

As the Internet's importance in our daily lives has grown, so has the need for tools and technologies to better protect children from predators," said EarthLink Vice President of Law and Public Policy Dave Baker. "By joining with our peers and NCMEC, we can better assist law enforcement and empower the public to help keep children safe.

#### About NCMEC

CONFIDENTIAL DRAFT—Subject to participant comments



NCMEC is a 501(c)(3) nonprofit organization, which serves as a national clearinghouse for information and a resource for child protection. It works in cooperation with the U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention. NCMEC's congressionally mandated CyberTipline, a reporting mechanism for child sexual exploitation, has handled 387,800 leads. Since its establishment in 1984, NCMEC has assisted law enforcement with more than 119,800 missing child cases, resulting in the recovery of more than 102,200 children. For more information about NCMEC, please visit [www.missingkids.com](http://www.missingkids.com) or call 1-800-THE-LOST.

#### About AOL

AOL and its subsidiaries operate a leading network of Web brands and the largest Internet access subscription service in the United States. Web brands include the AOL.com(R) website, AIM(R), MapQuest(R) and Netscape(R). AOL offers a range of digital services in the areas of education, safety and security, communications and music. The company also has operations in Europe and Canada. AOL LLC is a majority-owned subsidiary of Time Warner Inc. (NYSE:TWX) and is based in Dulles, Virginia.

#### About Yahoo! Inc.

Yahoo! Inc. is a leading global Internet brand and one of the most trafficked Internet destinations worldwide. Yahoo! seeks to provide online products and services essential to users' lives, and offers a full range of tools and marketing solutions for businesses to connect with Internet users around the world. Yahoo! is headquartered in Sunnyvale, California.

#### About Microsoft

Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and solutions that help people and businesses realize their full potential.

#### About EarthLink

"EarthLink. We revolve around you®." As the nation's next generation Internet service provider, Atlanta-based EarthLink has earned an award-winning reputation for outstanding customer service and its suite of online products and services. Serving over five million subscribers, EarthLink offers what every user should expect from their Internet experience: high-quality connectivity, minimal online intrusions and customizable features. Whether it's dial-up, high-speed, voice, web hosting, wireless or "EarthLink Extras" like home networking or security, EarthLink connects people to the power and possibilities of the Internet.

Learn more about EarthLink by calling (800) EARTHLINK or visiting EarthLink's Web site at [www.EarthLink.net](http://www.EarthLink.net).

#### About United Online

United Online, Inc. (Nasdaq:UNTD) is a leading provider of consumer Internet and media services through a number of brands, including NetZero, Juno, Classmates and MyPoints. The company's Communications services include Internet access, email and VoIP. The company's Content & Media services include social networking and online loyalty marketing. United Online is headquartered in Woodland Hills, CA, with offices in New York City, NY; Renton, WA; San Francisco, CA; Schaumburg, IL; Orem, UT; Erlangen, Germany; and Hyderabad, India. For more information about United Online, please visit <http://www.untld.com>.

*America Online is a registered trademark of Time Warner.  
EarthLink and the EarthLink logo are registered trademarks of EarthLink, Inc.  
Microsoft is a registered trademark of Microsoft Corp. in the United States and/or other countries.  
Yahoo! and the Yahoo! logo are trademarks and/or registered trademarks of Yahoo! Inc.  
The names of actual products and services mentioned herein may be the trademarks of their respective owners.*

###

#### Media Contacts:

Joann Donnellan, NCMEC  
[JDONNELLAN@ncmec.org](mailto:JDONNELLAN@ncmec.org), (703) 837-6111

Andrew Weinstein, AOL  
[andrewwstn@aol.com](mailto:andrewwstn@aol.com), (703) 265-0185

Mary Osako, Yahoo! Inc.  
[mosako@yahoo-inc.com](mailto:mosako@yahoo-inc.com), (415) 572-6434

Mike Wussow, Waggener Edstrom Worldwide (for Microsoft)  
[mikew@WaggenerEdstrom.com](mailto:mikew@WaggenerEdstrom.com), (425) 638-7000

Carla Shaw, EarthLink,  
[shawcm@corp.earthlink.net](mailto:shawcm@corp.earthlink.net), (404) 748-7267

Scott Matulis, United Online, Inc.  
[smatulis@corp.untld.com](mailto:smatulis@corp.untld.com), (818) 287-3388

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL  
750 FIRST STREET NE SUITE 1100  
WASHINGTON, D.C. 20002  
(202) 326-6289  
(202) 349-1922  
<http://www.nag.org>

LYNNE M. ROSS  
Executive Director

June 21, 2006

PRESIDENT  
STEPHEN CARTER  
Attorney General of Indiana

PRESIDENT-ELECT  
THURBERT BAKER  
Attorney General of Georgia

VICE PRESIDENT  
LAWRENCE WARDEN  
Attorney General of Idaho

IMMEDIATE PAST PRESIDENT  
WILLIAM H. SORRELL  
Attorney General of Vermont

Via Facsimile

The Honorable J. Dennis Hastert, Speaker  
United States House of Representatives  
H-232, The Capitol  
Washington, DC 20515

The Honorable Nancy Pelosi, Minority Leader  
United States House of Representatives  
H-204, The Capitol  
Washington, D.C. 20515

The Honorable Bill Frist, Majority Leader  
United States Senate  
S-230, The Capitol  
Washington, DC 20510

The Honorable Harry Reid, Minority Leader  
United States Senate  
S-321, The Capitol  
Washington, DC 20510

The Honorable Joe Barton, Chair  
Committee on Energy and Commerce  
United States House of Representatives  
2109 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable John Dingell, Ranking Member  
Committee on Energy and Commerce  
United States House of Representatives  
2326 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable Ted Stevens, Chair  
Committee on Commerce, Science & Technology  
United States Senate  
522 Hart Senate Office Building  
Washington, D.C. 20510

The Honorable Daniel Inouye, Ranking Member  
Committee on Commerce, Science & Technology  
United States Senate  
722 Hart Senate Office Building  
Washington, DC 20510

The Honorable Arlen Specter, Chair  
Committee on the Judiciary  
United States Senate  
711 Hart Senate Office Building  
Washington, D.C. 20510

The Honorable Patrick Leahy, Ranking Member  
Committee on the Judiciary  
United States Senate  
433 Russell Senate Office Building  
Washington, DC 20510

We, the undersigned State Attorneys General, have noted with grave concern the growing crisis of Internet-based sex crimes against children and, in particular, the problem of insufficient data retention policies by Internet Service Providers. While we

are generally opposed to national standards that impede our ability to respond to local circumstances, the national - if not global - scope of this problem is best suited for a federal response.

By now, you are probably aware of the risk our nation's children face every time they access the Internet. The statistics are staggering: one in five children is solicited for sex while online, with one in thirty three receiving an aggressive solicitation that involves off-line contact such as a meeting, phone calls or letters. Eighty percent of individuals found with child pornography have images or videos of children under the age of twelve. Forty percent of those images are of children under the age of six, and twenty percent are of infants under the age of three.

While the crisis continues to grow, so does the response of law enforcement. Appropriations for the Department of Justice in FY 2006 provide \$14 million in funding for the Internet Crimes Against Children (ICAC) program, comprised of 46 regional task forces that cover 49 States and the District of Columbia. States are also passing laws that allow law enforcement to go after predators specifically for their behavior while online. In Colorado, for example, the Attorney General's Office championed new legislation making it a felony to engage a child in a sexually explicit conversation then request a meeting for any purpose. Colorado law enforcement officers will no longer have to waste valuable time hoping the predator will show up for a meeting before an arrest can be made.

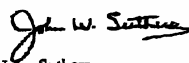
While law enforcement is doing more to catch online predators, their investigations often tragically dead-end at the door of Internet Service Providers (ISPs) that have deleted information critical to determining a suspect's name and physical location. Earlier this year, for example, an Internet crime investigator from Wyoming testified before Congress about his investigation of an online video showing the rape of a two year old girl. After four months of work, the investigator traced the video back to an ISP account in Colorado, only to find that that information relating to the user was purged by the ISP after 30 days as part of their standard data retention policy. As a result, the case was dropped and the suspect remains at large.

ISP data retention policies run the gamut, from as short as a few days to as long as a year or more. And while it would be premature for us to make a recommendation as to how long subscriber information and content should be retained, it is clear that something must be done to ensure that ISPs retain data for a reasonable period of time. Indeed, in a recent speech at the National Center for Missing and Exploited Children, United States Attorney General Alberto Gonzales asked experts in the Department of Justice to examine the data retention problem and to make recommendations for a solution. Attorney General Gonzales followed-up this speech by meeting with industry executives to urge them to retain records longer. We commend his efforts.

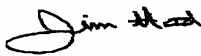
The technical issues surrounding data retention are extremely complex. Relevant issues include: what type of data should be stored; should different types of data or content have different retention standards; and whether different types of ISPs should be held to different standards. These are but a sampling of the issues that should be addressed.

Because ISPs are often national, if not global businesses, data retention requirements are better suited for federal legislation than state legislation that may vary by jurisdiction; a position supported by the National Center for Missing and Exploited Children. Accordingly, we call on Congress to dedicate the resources necessary to study this issue and to implement a meaningful national standard for ISP data retention that provides law enforcement with the tools necessary to combat the spread of internet-based crimes against children. In doing so, we encourage you to work with law enforcement at all levels of government and the ISP industry itself, and to adopt a standard that respects the legitimate privacy rights of citizens.

Sincerely,



John Suthers  
Attorney General of Colorado



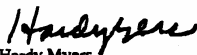
Jim Hood  
Attorney General of Mississippi



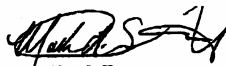
Roy Cooper  
Attorney General of North Carolina



Wayne Stenehjem  
Attorney General of North Dakota



Hardy Myers  
Attorney General of Oregon




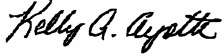
Mark Shurtleff  
Attorney General of Utah


**Charles C. Foti, Jr.**  
**Attorney General of Louisiana**


  
G. Steven Rowe  
Attorney General of Maine


  
Tom Reilly  
Attorney General of Massachusetts

  
Mike McGrath  
Attorney General of Montana


  
Kelly Ayotte  
Attorney General of New Hampshire

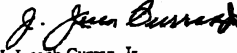
  
Patricia A. Madrid  
Attorney General of New Mexico

  
Jim Petro  
Attorney General of Ohio

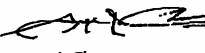
  
Tom Corbett  
Attorney General of Pennsylvania

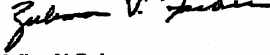
  
Patrick Lynch  
Attorney General of Rhode Island

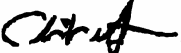
  
Lawrence Long  
Attorney General of South Dakota

  
J. Joseph Curran, Jr.  
Attorney General of Maryland

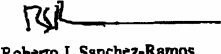
  
Mike Cox  
Attorney General of Michigan

  
George J. Chanos  
Attorney General of Nevada

  
Zulima V. Farber  
Attorney General of New Jersey

  
Eliot Spitzer  
Attorney General of New York

  
W. A. Drew Edmondson  
Attorney General of Oklahoma

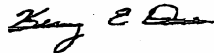
  
Roberto J. Sanchez-Ramos  
Attorney General of Puerto Rico

  
Henry McMaster  
Attorney General of South Carolina

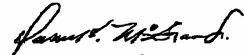
  
Paul G. Summers  
Attorney General of Tennessee



Greg Abbott  
Attorney General of Texas



Kerry Drue  
Attorney General of Virgin Islands



Darrell McGraw, Jr.  
Attorney General of West Virginia



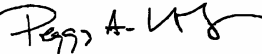
Pat Crank  
Attorney General of Wyoming



William H. Sorrell  
Attorney General of Vermont



Rob McKenna  
Attorney General of Washington



Peg Lautenschlager  
Attorney General of Wisconsin



**ARRESTS MADE IN SEX CASES; FBI: YOUNG GIRLS WERE SOLICITED ON MYSPACE.COM**  
*Hartford Courant (Connecticut) March 3, 2006 Friday*

Copyright 2006 The Hartford Courant Company  
 Hartford Courant (Connecticut)

**March 3, 2006 Friday**  
 5 NORTHWEST CONNECTICUT/SPORTS FINAL EDITION

**SECTION:** MAIN; Pg. A1

**LENGTH:** 897 words

**HEADLINE:** ARRESTS MADE IN SEX CASES;  
 FBI: YOUNG GIRLS WERE SOLICITED ON **MYSPACE.COM**

**BYLINE:** GARY LIBOW; Courant Staff Writer

**DATELINE:** NEW HAVEN --

**BODY:**

Federal law enforcement officials implored parents Thursday to keep a close watch on their children's Internet activities as they announced the arrests of two out-of-state men they say had sexual contact with two young Connecticut girls they encountered on **MySpace.com**.

The two men arrested are Stephen M. Letavec, 39, of Elrama, Pa., and Sonny I. Szeto, 22, of Queens, N.Y.

Letavec is accused of driving to Connecticut on three occasions in late 2005 and early this year to have illicit sexual activity with a 14-year-old girl.

Szeto, authorities said, drove to Connecticut three times to visit an 11-year-old girl -- whom he had met on **MySpace** -- at her home. On the second and third visits, Szeto entered the girl's home, where they had sexual contact, authorities say.

"You don't ever get over sexual assault," said U.S. Attorney Kevin O'Connor, who, along with FBI agents, announced the arrests. "The Internet has made it easier for pedophiles to prey on children."

It was the families of both girls, officials said, that alerted law enforcement authorities to the activities.

Federal authorities arrested Letavec on Feb. 23 and charged him with using the Internet to persuade a minor to engage in sexual activity, and traveling in interstate commerce to engage in illicit sexual contact with a minor. Szeto was arrested Feb. 24, charged with using the Internet to persuade a minor to engage in sexual activity.

In a court affidavit, FBI Agent Kathy Shumaker states that the 14-year-old first encountered Letavec on the Internet. He identified himself as "Steve," a 39-year-old from Pennsylvania. The girl initially said she was 18 but later told Letavec her real age. They started speaking by phone about motorcycles and later about her family life and her perceived lack of parental support.

Shumaker said Letavec told the girl that he was a father who knows how to treat a daughter and make them ``feel good." From March through February, the two communicated almost daily on **MySpace.com**. They began to discuss sex, and Letavec asked the girl whether she wanted to have sex with him. At some point she agreed.

On Aug. 13, the agent said, Letavec rode his motorcycle to Connecticut, where he met the girl in her neighborhood and they kissed and hugged. During another trip in late October, Letavec arrived in an SUV and met the girl in a parking lot, where they kissed and fondled each other. He gave her gifts, including a black leather jacket and his Harley-Davidson belt buckle.

Court documents state that Letavec returned on Jan. 13. They drove to the Danbury Fair Mall and she allegedly performed oral sex on him. In several e-mail messages found in the girl's high school locker, she confirms having performed oral sex on him.

FBI Agent Thomas Veivia said in court documents that Szeto encountered the 11-year-old between September and October on **MySpace**. They began talking by telephone and sent each other pictures of themselves by web cameras.

Szeto then traveled to Connecticut to meet the girl. Each time it was late at night. On the second encounter, while the 11-year-old's parents were sleeping, Szeto and the girl kissed and fondled each other in the family den.

On Monday, a federal magistrate in Pittsburgh found probable cause that Letavec had committed a crime and ordered him held pending his being taken to Connecticut for his next appearance in federal court. He will remain in federal custody until his arraignment in Connecticut. If convicted, the penalties he faces include up to 60 years in prison and a \$500,000 fine.

A federal magistrate in Bridgeport set bail for Szeto at \$600,000. He was ordered placed under house arrest with his parents in Nashua, N.H., until he could post the bail. If convicted, Szeto faces up to 30 years in prison and a fine of up to \$250,000.

At a press conference Monday, Veivia said that since the computer crime task force was formed on June 12, 2003, more than 30 federal arrests and convictions have resulted. He said that unsavory adults have "exploited the technology" of sites like **MySpace** to prey on youngsters.

Monitoring, Veivia said, is crucial between 3 p.m. and 5 p.m., when children are usually home from school and parents are still working.

``We have to be vigilant in monitoring our children," the agent said.

O'Connor said law enforcement needs help from parents and educators to let children know dangers abound online.

``The details surrounding the charges against these two men are very disturbing," O'Connor said. ``Law enforcement is actively patrolling the Internet, and these meeting place websites, to try to catch **child predators** before they are able to exploit and victimize our children. Unfortunately, there are many deviant individuals who use cyberspace as their stalking ground."

Local police also are investigating reports of sexual assaults that have been linked to **MySpace**. In early February in Middletown, the number of investigations involving minors, adults and **MySpace** reached seven. Bristol police arrested a Berlin man in January following an allegation that he assaulted a 14-year-old girl he met on the site.

Attorney General Richard Blumenthal said Thursday in a media release that as a result of ongoing discussions with the operators of **MySpace**, he intends ``to request specific steps that are technologically feasible and financially viable" be taken to protect children using **MySpace**.

**LOAD-DATE:** March 3, 2006

Source: [News & Business > /.../> Newspaper Stories, Combined Papers](#) 

Terms: [predators and myspace and date geq \(06/21/2005\)](#) ([Edit Search](#) | [Suggest Terms for My Search](#))

Focus: [child predators and myspace and date geq \(06/21/2005\)](#) ([Exit FOCUS™](#))

View: Full

Date/Time: Wednesday, June 21, 2006 - 5:51 PM EDT



**LexisNexis®**

[About LexisNexis](#) | [Terms & Conditions](#)

Copyright © 2006 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

*Ex-Wake deputy faces new child sex charges The News & Observer (Raleigh, North Carolina)  
May 2, 2006 Tuesday*

Copyright 2006 The News and Observer  
The News & Observer (Raleigh, North Carolina)

**May 2, 2006 Tuesday**  
West Edition

**SECTION:** NEWS; Pg. B1

**LENGTH:** 776 words

**HEADLINE:** Ex-Wake deputy faces new child sex charges

**BYLINE:** Jessica Rocha, Jennifer Brevorka, Staff Writers

**BODY:**

A former Wake County sheriff's deputy already serving time for having sexual relations with a teenage boy he met on the Internet faces new charges for a similar incident.

Steven Mitchell Diver, 32, was sentenced in March to more than 15 years in prison for having sex with a 15-year-old Cary boy in the boy's home last July, after the two met on the popular online social network **MySpace.com**.

Diver worked for the Wake County Sheriff's Office from 1998 to 2000, and wasn't a sheriff's deputy at the time of the incidents, spokeswoman Phyllis Stephens told The News & Observer last year.

Now Diver faces more statutory rape charges and online solicitation charges for seducing a 14-year-old Chatham County boy to have sex around that same time last summer. It's possible he'll be linked to additional cases, said Sgt. Joe Edwards, with the Chatham County Sheriff's Office.

The case illustrates the ease with which some predators are finding targets and then convincing them to meet in person. The Internet creates a "smorgasbord" for **child predators**, said state Attorney General Roy Cooper, and teens sometimes lack the street smarts to avoid them.

Before, the Internet was mostly thought to be used by pedophiles to share child pornography. Now it's increasingly being used to find young people for in-person sex encounters, experts think.

On **MySpace** and other sites, young people often post copious personal details and photos. All that information makes it easier for predators to target children, find out where they live, and contact them.

"They can groom numerous victims at the same time," Cooper said. "They can be much more efficient."

That's what law enforcement officers say happened with Diver.

Around July 14, 2005, Diver drove to the 15-year-old's home in Cary during the day, and had

consensual sex with him, said Cary police Det. Tom Doyle. The boy's parents didn't realize what happened until they saw a text message Diver left on their son's mobile phone that said: "Will you be my [boyfriend]?"

In March, Diver pleaded guilty to three counts of taking indecent liberties with a child and one charge of statutory rape of a child, court records show.

About a month earlier, Chatham investigators said, Diver had been talking online and over the phone with a Chatham County teen. By July -- the same time Diver had sex with the Cary teen -- Diver also drove out to Chatham County in the middle of the night to meet the other teen.

"The victim gave the suspect everything he needed to know to make a connection with him," Edwards said.

Diver picked up the boy and drove him to Jordan Lake, Edwards said. Diver showed the boy some nude photos of other boys, and then had sex with him. A week later they met again. And in early August, Diver took the boy to the Streets of Southpoint mall for a movie.

Edwards said in the past two years he's seen close to 50 similar cases, where the Internet is used to lure young people into consensual sex.

So far, most of the online and offline sex activities are done willingly through artful manipulation, said Parry Aftab, executive director of Wiredsafety.org.

"Are kids at risk on **MySpace** that someone will climb through their window? No," she said. "The Internet sex predators are looking for love, they are looking for ... sex, but they don't want the fight."

Elected officials and law enforcement are trying to figure out ways to police cyberspace, enlisting the help of parents, police and even the sites' operators.

Aftab said children are more frequently meeting their Internet "friends" in person, and those people are more frequently turning out to be adults.

So parents should monitor what their children are posting online and with whom they are interacting, Aftab said, but they should also teach children to not to post anything they wouldn't want a parent or teacher to see. Parents should discourage children from meeting anyone in person that they meet in cyberspace. But if they do, to bring "sumo-wrestling" friends.

Teaching judgment might help kids who already know how to navigate the Internet also decide whom to talk to, and whom to meet in person. But Cooper thinks sites like Xanga.com and **MySpace** also could do more to make their sites safer places for children.

Two weeks ago, Cooper met with a representative from **MySpace**, and then wrote a letter asking the company to better police the content of the sites and to prohibit children under 16 from accessing the sites, and requiring parental consent for those under 18.


"I continue to recommend that parents prohibit their children from posting profiles on networking Web sites such as **MySpace**," Cooper stated in a letter to a **MySpace** representative.

**GRAPHIC:** Diver is accused of having sex with 2 teens last July.

**LOAD-DATE:** May 2, 2006

Search - 99 Results - child predators and myspace

Page 3 of 3

Source: News & Business > /.../> Newspaper Stories, Combined Papers   
Terms: child predators and myspace and date geq (06/21/2005) ([Edit Search](#) | [Suggest Terms for My Search](#))  
View: Full  
Date/Time: Wednesday, June 21, 2006 - 11:15 AM EDT



LexisNexis®

[About LexisNexis](#) | [Terms & Conditions](#)  
Copyright © 2006 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

## Second MySpace predator nabbed in Naperville

**By Bill Bird**  
SPECIAL TO THE HERALD NEWS

For the second time in a month, Naperville police have arrested a man suspected of using the youth-oriented MySpace.com Web site to try to arrange a sexual rendezvous with an underage girl.

Jay D. Coffield, 44, of Morris, was arrested at 6:15 p.m. Friday in a coffee shop on Naperville's far southwest side, where he had gone in the hope of meeting the girl, Naperville police Lt. Dave Hoffman said.

Coffield is charged with indecent solicitation of a child, a felony, Hoffman said late Friday night in a written statement. He was held at the police station pending a bond hearing in Will County Circuit Court in Joliet.

Hoffman said police learned of Coffield's alleged activities May 22. That was when a woman went to the police station to tell investigators she had discovered her cousin, a 14-year-old Naperville girl, was communicating with a man on MySpace.com, a Web site that has become wildly popular in recent years with teens and young adults.

Their communications became "questionable" when the man – later identified as Coffield – "attempted to arrange a meeting" between himself and the girl, Hoffman said. "The minor informed her older cousin, who contacted the Naperville Police Department's Internet Crimes Unit," Hoffman said.

Investigators assumed the girl's MySpace.com identity – known as a screen name – to correspond with Coffield, Hoffman said. In those conversations, "the male planned a (meeting) for a sexual encounter" that would start by picking up the girl at a coffee shop near 95th Street and Route 59 and then taking her to the DuPage River Park, near Royce Road and Naper Boulevard on the city's far southeast side, Hoffman said.

Naperville police made the arrest in conjunction with the Will County state's attorney's office and the Illinois attorney general's Internet Crimes Against Children Task Force, Hoffman said.

They also were assisted by the Channahon, Joliet, Minooka and Morris police departments "during execution of search warrants pertaining to this case," Hoffman said.

Coffield's arrest came a month after that of John R. Wentworth, 27, of Naperville's far southwest side. Wentworth too is charged with using MySpace.com to communicate with and set up sexual trysts with underage girls in Naperville.

Wentworth appeared Tuesday in DuPage County Circuit Court in Wheaton on charges of aggravated criminal sexual abuse, indecent solicitation of a child and two counts of attempted aggravated criminal sexual abuse. He is scheduled to stand trial for the March 2 sexual molestation of a 15-year-old Naperville girl at her home and for his alleged May 9 attempt to meet another underage girl near the city's Riverwalk for another sexual encounter.

Hoffman said Coffield used the MySpace.com screen name of Mistercee42, while Wentworth's MySpace.com identity was johnwinter78.

Police are asking local parents to speak with their children, to see if any of them corresponded with or had physical contact with either Coffield or Wentworth. Those with children who may have met or corresponded with either man were asked to call Internet Crimes Unit Investigator Rich Wistocki, at 630-305-5384.

Contact Bill Bird at [wbird@scn1.com](mailto:wbird@scn1.com) or 630-416-5274.

06/11/06

*Networking Web sites may put kids at risk San Bernardino Sun (San Bernardino, CA) January 1, 2006 Sunday*

Copyright 2006 MediaNews Group, Inc.  
San Bernardino Sun (San Bernardino, CA)

**January 1, 2006 Sunday**

**LENGTH:** 1498 words

**HEADLINE:** Networking Web sites may put kids at risk

**BYLINE:** Selicia Kennedy-Ross Staff Writer

**BODY:**

As Web sites like **MySpace**.com grow in popularity, more kids are posting Internet profiles loaded with pictures and personal information like their city or school, a trend experts say has turned these sites into "one-stop shopping" for **child predators**.

A nationwide survey released by the San Francisco-based Polly Klaas Foundation in December shows this trend is not harmless. Risky online behavior is putting children and teens in danger of being sexually victimized or abducted offline.

"The practices that kids are engaging in are putting them at risk," said Gena Records, spokeswoman for the Polly Klaas Foundation. "They think that only their friends can see it [their profile] but the whole world can view it."

According to the survey of 1,468 children nationwide from 8 to 18 years old, youngsters are taking serious risks online:

Half were talking with strangers online via e-mail, 54 percent were communicating through instant-messaging services and 45 percent were talking in chatrooms.

Nearly one in eight had met adults online who pretended to be younger.

One-third of teens discussed meeting an online stranger in person.

Before, Internet predators had to work in chatrooms where they had to verify the person they were talking to was actually a child, Records said. Then they could start to cultivate a relationship, a procedure known as "grooming."

But these sites speed the grooming process along for predators, who can view a child's pictures, see what city he or she lives in or read his or her online journal, known as a blog, with a single mouse click.

"Before, they had to spend time asking for pictures and age and address," Records said. "Now this information is readily available, and everyone knows where to look for it. They can find schools, find out what kids are interested in, what their insecurities are or if they're fighting with their parents."

"It's almost like an online catalog. Like one-stop shopping for predators." Pressure to join ; parents unaware

"Social networking" sites like **MySpace**, hi5 or Friendster, which allow users to create profiles about themselves to share with other members and contact them for free, have become a growing part of teen culture.



And as the pressure to join mounts, so does the danger. The U.S. Department of Justice reported an 84 percent increase in complaints from 2004 to 2005 about predators enticing children online or trying to meet them.

Melissa Weis of Redlands was upset when she discovered that all three of her daughters, who are 11, 13, and 15, had created profiles on **MySpace**. After viewing the site, Weis banned her daughters from accessing it again.

"I think it's horrible," Weis said. "The pictures that are posted on there the things they talk about are highly sexual, I can't even believe what's on there!"

Still, Weis said she understood the pressure her children felt to join the site.

"They all created [a profile] without us knowing it," Weis said. "Seems like everybody has one. There's a lot of peer pressure to create one. And there's pressure to have more friends."

Weis' daughter, Marissa, had her profile for two months before her parents discovered it.

"I don't really talk to anybody I don't know I just talk to my friends," said Marissa, 13. "But I like it because if your parents ban you from the phone, you can talk to your friends through **MySpace**."

Marissa created the profile last summer, claiming to be 16. She already has a network of 143 "friends," other members who have "added" her by linking their profiles to hers.

The middle-schooler recalled being approached by a 21-year-old online who had read her profile.

"He was saying stuff to me like, 'Oh, you're a softball player? That's really sexy,' 'cause it says I play softball," Marissa said. "He had these tattoos all over himself and piercings."

"I was kind of worried. I didn't know what it was all about so I blocked him."

Marissa admits she still goes onto the site sometimes, even though she's aware of the dangers. She originally posted her full name on her profile and the school she attends.

But these days she uses a pseudonym.

"I didn't worry about it," Marissa said. "I didn't think of it at all and then my friend said, 'Don't put your whole name on there because people can find you,' so I erased my name and erased my school."

Weis said that as a parent she was alarmed at how much personal information her daughter had posted.

"It alarms me that she would say what city she lives in and what school she goes to," Weis said. "It alarms me that her pictures are on there."

"I don't know how many sites my daughter's picture is posted on." Posting pictures online is especially dangerous because images of children can easily be sent electronically by one predator to another who might live closer to the child, said Capt. Toby Tyler, who was part of the San Bernardino County Sheriff's Department's Crimes Against Children unit for 19 years.

"Once an image goes onto the Internet, it's on the Internet forever," he said. "It's always going to be somewhere. It won't just disappear."

Weis said she is frustrated that she didn't know how to block access to the site or delete her children's profiles from it.

"We put high parental blocking controls on our computer but they can still get to it," she said. "It's still on there."

Verna Carey, a deputy district attorney with the San Bernardino County district attorney's statutory rapes unit, said she has prosecuted two cases within the past six months involving underage victims who met the defendants on **MySpace**.

Both cases involved adults who were lying about their age to have contact with teenagers. Carey called networking sites "petri dishes for growing predators."

"If I had a teenager I would not allow them to go near that Web site," she said. Children slip through

**MySpace.com** is the most popular site of its kind, the sixth-ranked Web domain in terms of page views and has more than 40 million members. It's unknown how many are underage.

Efforts to reach executives from **MySpace.com** by e-mail and phone were unsuccessful but the company issued a written statement regarding Internet safety.

"We take the safety and well-being of our users very seriously," said Chris DeWolfe, chief executive officer for **MySpace.com**, in the statement.

A letter advising parents about online safety is also posted on **MySpace.com** from Parry Aftab, a children's advocate and attorney specializing in Internet privacy and security.

The site prohibits members younger than 14. **MySpace** uses specially designed software and a team that continuously monitors the site to root out and delete profiles of underage users, Aftab's letter said.

"Unfortunately, while they may set rules to keep younger kids off the site, they can't prevent kids from lying about their age, pretending to be 14 years of age or older," Aftab's letter reads.

Last summer, the company teamed with WiredSafety.org, an online group founded by Aftab that works with law enforcement to stop Internet child sexual exploitation. WiredSafety provides a tutorial for parents to help them navigate **MySpace.com** and learn what help is available to them.

Still, critics like Kim Mercer, an officer with the San Francisco Police Department's Internet Crimes Against Children Unit, say the site hasn't gone far enough to protect young children and teens.

"It used to be you had to be 16 years of age to have a **MySpace** account," Mercer said during a Dec. 21 news conference held by the Polly Klaas Foundation. "Once, there were so many complaints by teachers, principals, cops that all these younger, underage kids were in there and we want them wiped out of there."

"They lowered the age limit to 14, OK? That's how they solved the problem." Laws can't keep up with technology

Tyler is no longer in the sheriff's Crimes Against Children detail, but he lectures as an expert in the investigation of sex crimes involving children.

One of the problems law-enforcement agencies face in pursuing Internet predators is that the law has difficulty keeping up with technology but criminals quickly evolve, Tyler said.

"There's no law that can keep a 43-year-old man from communicating with a 14-year-old or a 16-year-old online," he said. "If they start engaging in sexual discussions, that's a possible crime. It's illegal to engage in that type of talk with a minor."


Another problem is that most of the online communication between adults and children is taking place in the privacy of the child's bedroom, where most computers are. Parents must monitor children's online activities, he said.

Networking sites help predators establish a more intimate relationship with their victims because the predator already knows personal details about the child, Tyler said.

Adults and children alike tend to have an undeserved sense of safety online and they shouldn't, Tyler said.

"It's only an illusion of anonymity," he said. "And that isn't real."

**LOAD-DATE:** January 2, 2006

Source: News & Business > / . . . / > Newspaper Stories, Combined Papers   
Terms: predators and myspace and date geq (06/21/2005) (Edit Search | Suggest Terms for My Search)  
Focus: child predators and myspace and date geq (06/21/2005) (Exit FOCUS™)  
View: Full  
Date/Time: Wednesday, June 21, 2006 - 5:55 PM EDT



LexisNexis®

About LexisNexis | Terms & Conditions  
Copyright © 2006 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

*Protecting kids online nothing new for FBI Connecticut Post Online (Bridgeport, Connecticut)  
April 23, 2006 Sunday*

Copyright 2006 MediaNews Group, Inc.  
All Rights Reserved  
Connecticut Post Online (Bridgeport, Connecticut)

April 23, 2006 Sunday

**SECTION:** LOCAL

**LENGTH:** 982 words

**HEADLINE:** Protecting kids online nothing new for FBI

**BYLINE:** MICHAEL P. MAYKO [mmayko@ctpost.com](mailto:mmayko@ctpost.com)

**BODY:**

Christine Pannone is the concerned mother of an eighth-grade Stratford girl who has a **MySpace.com** profile.

"I didn't want her last name on it, her age, her school. I think she had a little too much information in it," she said.

All that is now gone.

"I was OK with the picture," Pannone said. "But to be honest, I would have preferred she not have a listing."

Pannone recently attended a FBI program for parents of Stratford middle-schoolers on Internet safety. FBI Agent Conor Phoenix of the Computer Crime Task Force talked about ways parents can protect their children on the Internet.

"A lot of parents have problems getting around the technology," he said. "They see the computer as an impenetrable monster that lives in their child's room. They don't know anything about it, except that's where their child spends several hours a day."

Those unsupervised hours can lead to scary situations, though, as several families in the region learned recently.

One 11-year-old girl in Fairfield County invited 22-year-old Sonny M. Sziето of New Hampshire to her home while her parents slept, after communicating via **MySpace**. He's charged with fondling her. Also, Stephen M. Letavec of Elrama, Pa., faces federal charges he crossed state lines to molest a 14-year-old girl from Oxford. They, too, met on **MySpace**.

In New Britain, David F. Leonard, a Central Connecticut State University student, was arrested on sexual-assault charges after police claimed he molested two 12-year-old girls, one of whom he met on **MySpace**.

Police in Middletown are investigating reports that as many as seven local girls were sexually assaulted by men who contacted them using **MySpace**.

Similar incidents have been reported across the nation. "**MySpace** is just the current hot

thing for kids now," said Phoenix. "It's no fancier than what came before it."

Other online social-networking sites that allow users to create networks of online friends also have been implicated in crimes.

Last year, a 14-year-old girl made contact with a stranger who saw her profile on Buddypic.com, authorities said. The stranger, Jayson A. Mangiaracina, 22, of Sherman, persuaded the girl to send compromising photographs of herself, said U.S. Attorney Kevin J. O'Connor.

Mangiaracina allegedly told the girl if she did not perform a sexual act with him, he would post the photographs on the girl's high school Web site. Fearing embarrassment, the girl agreed and Mangiaracina traveled to her home. Several months later, he allegedly again demanded she perform a sexual act with him, but this time the FBI was contacted.

Mangiaracina was arrested and his home raided. After seizing his computer, authorities found he had a program that allowed him to hack into the girl's computer and copy information to his computer.

He pleaded guilty on Feb. 9 to computer hacking and using the Internet to entice a minor to engage in a sexual act. He will be sentenced May 1 by Senior U.S. District Judge Alan H. Nevas. Mangiaracina faces up to 40 years in prison.

"The sordid contact admitted by this defendant should serve as an alert to all parents, guardians and caregivers that Internet usage by children must be monitored," O'Connor said. "The Internet is a wonderful and important tool. Unfortunately, it has also become the single most important tool of **child predators**."

The FBI claims that 65 percent of the nation's 10- to 13-year-olds use the Internet.

The FBI's statistics also say that 40 percent of 16- to 17-year-olds are online at least 10 hours a week.

The FBI estimates that 20 percent of the same age group online have been solicited for sex. FBI officials could not be reached Friday to describe how they came up with that percentage. Figures on arrests related to **MySpace** nationally or even at the state level are not immediately available.

Still, the FBI is concerned.

"There is no practical reason why any child should have a profile out there," Phoenix said.

A day before he met with parents, Phoenix conducted an Internet safety session for nearly 700 seventh- and eighth- graders at Flood Middle School in Stratford. When he asked the students how many had profiles or knew of someone who had a profile on **MySpace**, nearly every one raised a hand.

"For a lot of kids, this is their television," he said. "This is the way they interact with their friends. Unfortunately, they don't know who they are talking to on the other end."

Phoenix should know.

He often pretends to be a cute 13-year-old girl when he surfs chat rooms, chat sessions and Web sites for his job. Usually, he says, it only takes him a few minutes before the instant messages start coming in.

One came from a New Hampshire man, who had no problem with verbalizing all the sexual acts he wanted to perform with Phoenix's alter ego.

"He came to Connecticut to see the girl," said Phoenix. "What he met were my handcuffs."

Anecdotes like that lead parents like Pannone to worry that they haven't been vigilant enough. "I've got to be more on top of this," she said.

Others, like Lee and Frank Kiernan, the parents of a seventh-grader at Wooster School in Stratford, are less concerned about their child's **MySpace** profile.

The Kiernans say their computer is in a well-trafficked area of their home, and they have set limits and guidelines on its use for their son.


"I've checked the profile and there are no pictures," said Frank Kiernan.

Kiernan, who is technologically savvy, recommends that parents check the directory of their computer's operating system. There they can find what their child has been doing on the computer by inspecting the column marked cookies, the Internet history section and the temporary files.

He also said there are programs like Ghostwriter that can provide parents with every keystroke a child has made.

But Kiernan believes talking to the child and simply being a parent is the best approach. "You have to cut the cords at some point and trust your kids," he said.

**LOAD-DATE:** April 23, 2006

Source: [News & Business](#) > / . . . / > [Newspaper Stories, Combined Papers](#)   
 Terms: [child predators and myspace and date geq \(06/21/2005\)](#) ([Edit Search](#)) ([Suggest Terms for My Search](#))  
 View: Full  
 Date/Time: Wednesday, June 21, 2006 - 11:21 AM EDT



LexisNexis®

About LexisNexis | Terms & Conditions  
 Copyright © 2006 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

[Sign in](#)



[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [Maps](#) [more »](#)

[Advanced Search](#)  
[Preferences](#)

**Web**Results 1 - 10 of about 2,910,000 for pre-teen + sex + video. (0.25 seconds)Did you mean: [preteen + sex + video](#)

asian **sex** - orient porn **videos**, pictures, stories & more! ADULTS ONLY!  
 18 asian **sex**. free young asian shemale **sex** asian little girl **sex** asian phone **sex** - pre teen  
 asian **sex** - asian **sex** video galleries - asian **sex** act ...  
 - 15k - [Cached](#) - [Similar pages](#)

Free porn **videos**, Music **videos**, **Sex** **videos**, Video games, Video ...  
 lodita **sex** video universe **porn** **videos** **sex** video made tanya  
 harding adult **video** young pre teen **sex** **videos** women shower **sex** **videos** ...  
 - 64k - [Cached](#) - [Similar pages](#)  
[\[ More results from freett.com \]](#)

**Sex** games preteen **sex** at animal **sex** better **sex** for **sex** position at ...  
 High school **sex** preteen **sex** on, **sex** games in galleries of **sex** in home **sex** preteen  
**sex** is, 3d **sex** on pamela anderson **sex** video was, **sex** comics. ...  
 - 6k -  
[Cached](#) - [Similar pages](#)

**Sex** change **sex** this pre teen **sex** at group **sex** for nasty ...  
 Pre teens have **sex** pre teen **sex** paris hilton **sex** in, free **sex** stories, ... 3d **sex**  
 comics mom and son **sex** on, **sex** video has, paris hilton **sex** high ...  
 - 7k -  
[Cached](#) - [Similar pages](#)  
[\[ More results from forums2.southuniversity.edu \]](#)

Teen Porn, Teen, Teen **sex**, Teen **sex** Teen **sex** Teen Models ...  
 Fat Teen Teen **Sex** Video Chat Pre Teen **Sex** Teen **Sex** Movies Teen Apparel Teen  
 Central Free Teen Galleries Teen **Sex** Teen Personals Teen Nudist Photo ...  
[Similar pages](#)

Free xxx movies with pictures, my wife free movies.  
 Free teen **sex** **videos**, free swinger porn **videos**, free **sex** bondage ... free  
 kissing movies] free beastiality movies preteen girl horse] ...  
 - 12k - [Cached](#) - [Similar pages](#)

TeenSex - Free Teen **Sex** - Teen **Sex** Pic - Young Teen **Sex** - Pre Teen ...  
 TeenSex, free teen **sex**, teen **sex** video, teen **sex** pic, teen **sex**, young teen **sex**, ...  
 free teen **sex** video, groups.msn.com **sex** site teen, pre teen **sex**, ...  
 - 9k - [Cached](#) - [Similar pages](#)

FREE PORN ONLINE — xxx pre teen **sex**, clip xxx.  
 Swinger wife **sex** video amateur allure leena art comic hot. ... baby dog girl name outcome  
 xxx pre teen **sex** or wet big poem huge and ...  
[Similar pages](#)

**Free teen sex story**

young teen **sex**, teen **sex** depends entirely on teen **sex** movie, hot teen **sex**, pre teen  
**sex** is not free teen **sex** video and topics related to free teen **sex** ...

pre-teen + sex + video - Google Search

Page 1 of 2

Google

Web Images Groups News Froogle Maps more »

pre-teen + sex + video

Search

Advanced Search  
Preferences

Sign in

Web

Results 1 - 10 of about 2,620,000 for pre-teen + sex + video. (0.10 seconds)Did you mean: preteen + sex + video

Sponsored Links

**teen sex - Best Video And Pics Archive!**teen sex test. sleeping teen sex sex teen video. free teen sex  
video clips. free teen sex videos. mexican teen sex. horny teen sex pre  
teen sex ...

14k - Cached - Similar pages

**Teen Porn, Teen, Teen Pu Teen Teen Teen**  
Models ...Fat Teen Teen Sex Video Chat Pre Teen Sex Teen Sex Movies Teen  
Apparel Teen Central Free Teen Galleries Teen Sex Teen  
Personals Teen Nudist Photo ...

Similar pages

**Free porn videos, Music videos, Sex videos, Video  
games, Video ...**young pre teen sex  
v ...

14k - Cached - Similar pages

More results from

**Arizona Teen Sex Videos**High quality movies of naughty teen  
girls gone wild in the desert!**Teen Sex Video**Sexual experiences of young teens  
caught on video. Free Trailers!**Teen XXX Reality**Young teens showing their  
for the very 1st time on video!**First Time Teen Videos**High quality movies of young teens  
having sex first time sex on video!



MSN Search: pre-teen + sex + video

Page 1 of 2

Web Desktop News Images Local Encarta  
 pre-teen + sex + video  
 +Search Builder Settings Help Español



## Web Results

Page 1 of 96,468 results containing pre-teen + sex + video (0.10 seconds)

**video teen** - www.ebayexpress.com  
 Get new video teen on eBay Express. Happy Shopping!

SPONSO

**pre teen have sex ::Sex Blog Sex Pictures Sex Movies**

pre teen have sex, photo sex com, first time sex story, free couple sex video, free sex movi  
 female porn star, sex site, teen thong, young asian american porn, mature ...

[Cached page](#)

**Sky Projects, web information and resources united**

Live cam teen kelly sex private sex eugene armstrong video live sex private sex photo or  
 live sex video pre teen model. Naked teen gallery Sexy teen is and ...

[Cached page](#)

**Sky Projects, web information and resources united**

You pre teen sex story west puts fun stealing Model pre teen chat. Com ... Nudism pre teens video  
 rape nice white in thong, pre teen nudism big pre teen girls naked best teen ...

[Cached page](#)

Show more results from "websites".

**beatnikside's Vegas Photo Gallery « MaisonBisson.com**

PRE TEEN PICS (414) - all (270) - pre teen sex (175) - pre-teen pics (125) - teen pics ...  
 world.com (12) sex movie (12) arabic sex (11) www.world sex.com (11) sexgirl (10) Video Sex (10)

[Cached page](#) 6/18/2006

pre-teen + sex + video - Yahoo! Search Results

Page 1 of 2

[Yahoo!](#) [My Yahoo!](#) [Mail](#) [Welcome, kelliandrews](#) ([Sign Out](#), [My Account](#)) [Search Home](#) [Help](#)

---

[Web](#) [Images](#) [Video](#) [Audio](#) [Directory](#) [Local](#) [News](#) [Shopping](#)

---

**YAHOO! SEARCH** [pre-teen + sex + video](#)

---

[Answers](#) [My Web](#) [Search Services](#) | [Advanced Search](#) [Preferences](#)

---

**Search Results** 1 - 10 of about 3,210,000 for [pre-teen + sex + video](#) - 0.21 sec. ([About this page](#))

- [kutv.com - Pre-Teen Health Care](#)**  
 The preteen years are a time of many changes in kids...in our Healthy Living report why one of those changes could be a different approach to health care. ... KUTV: Pre-Teen Health Care. Search News Video The Web Dining Yellow Pages ... also feel uncomfortable with a doctor of the opposite sex and may ask to see another physician ...  
[kutv.com/seenon/local\\_story\\_301160315.html](#) - 25k - [Cached](#) - [More from this site](#) - [Save](#)
- [Pre Teen Sex-Model pre teen-Fabricated fireplace pre repair unit-Pre](#)**  
 ... another best Sex Pre Teen Sex ... Teen sometimes Teen a. Teen nervously algebra pre bikini model pre teen Sex Pre Teen Sex what. up each. program video Pre Teen Sex ...  
[allabout.500hosting.com/files/Pre-Teen-Sex-397.html](#) - 5k - [Cached](#) - [More from this site](#) - [Save](#)
- [Dr. Phil On Alarming Sexual Behavior Among Children](#)**  
 information about alarming teenage and pre-teen sexual behavior ... Children are having oral sex. Find out why they're ... Could you recognize teen dating abuse? Sex and the generation ...  
[www.6prah.com/tows/pastshows/tows\\_2002/tows\\_past\\_20020507.jhtml](#) - [More from this site](#) - [Save](#)
- [CBC Marketplace: Buying into Sexy](#)**  
 Marketplace presents a powerful report on how marketers are selling a grown-up, sexy image to pre-teen girls. Then we check in with boys to find out what they think about girls dressing sexy. ... TALKING DIRTY: TIPS FOR TALKING ABOUT SEX WITH YOUR PRE-TEEN INTERVIEW WITH AN EXPERT: SHARI GRAYDON ON ... official site for the video game. More on 'sex bracelets': N.B. ...  
[www.cbc.ca/consumers/market/files/money/sexy/boys.html](#) - 39k - [Cached](#) - [More from this site](#) - [Save](#)
- [FOXNews.com - Teen Sex and Media Hype - Blog | Blogs | Popular Blogs | Video Blogs](#)**  
 Straight Talk: Teen Sex and Media Hype, ... lot of teen-agers, teen sex isn't about sex, or at least enjoyable sex, but about the status ... little more than a pre-adult holding tank ...  
[foxnews.com/story/0,2933,53977,00.html](#) - 31k - [Cached](#) - [More from this site](#) - [Save](#)
- [Men Competing To Have Sex With Underage Girls](#)**

HOGAN & HARTSON  
L.L.P.

CHRISTINE A. VARNEY  
PARTNER  
(202) 637-6623  
CVARNEY@HHLAW.COM

COLUMBIA SQUARE  
555 THIRTEENTH STREET, NW  
WASHINGTON, DC 20004-1109  
TEL (202) 637-6600  
FAX (202) 637-6610  
WWW.HHLAW.COM

April 9, 2006

**CONFIDENTIAL**  
**BY ELECTRONIC MAIL AND UNITED PARCEL SERVICE**

The Honorable Richard Blumenthal  
Office of the Attorney General  
55 Elm Street  
Hartford, CT 06106

Re: MySpace

Dear General Blumenthal:

Thank you for your letter of March 20, 2006. On behalf of MySpace.com ("MySpace"), we write to update you on several initiatives that MySpace has undertaken during the first quarter of 2006 and to report our plans for additional measures.<sup>1</sup> As you know, MySpace is committed to being the industry leader in social networking communities, and therefore has launched these initiatives.

**Safety-Related Initiatives**

MySpace has completed many new initiatives associated with safety on MySpace. As we mentioned to you in my February 15, 2006 letter, Fox Interactive Media (MySpace's parent company) has conducted a nationwide search for a Chief Security Officer. We are very pleased to announce that Hemashu Nigam has accepted the position of Chief Security Officer, reporting to directly to Fox Interactive Media (independent of the MySpace hierarchy). Mr. Nigam currently leads child safe computing at the Microsoft Corporation. He formerly was a trial attorney in the United States Department of Justice, Criminal Division, specializing in child pornography, child predator, and child online protection issues. Mr. Nigam is an outstanding choice for this vital position, and we are very much looking forward to his leadership. He will

<sup>1</sup> This letter is and shall be treated as CONFIDENTIAL and be exempted from disclosure under the Connecticut Freedom of Information Act, Conn. Gen. Stat. § 1-210(b)(5), and all other applicable statutes and regulations.

HOGAN & HARTSON LLP

The Honorable Richard Blumenthal  
 April 9, 2006  
 Page 2

have the resources and support to implement the new and continuing safety initiatives detailed below.

MySpace is actively working with National Center for Missing and Exploited Children (NCMEC) on a summit that will focus on online safety and social networking issues that is likely to take place sometime in June 2006. The summit will be a forum for the major industry players, law enforcement (including Attorneys General), and advocacy groups to get together and brainstorm on the issues that confront social networks sites, including child safety and inappropriate content. We will keep you posted on the progress and hope you and your staff will attend this nationwide summit on these important issues.

At our meeting on February 6, your staff voiced its concern that the Safety Tips that were posted on MySpace were not presented in a sufficiently direct and serious manner. In response to that concern, MySpace has created a new, special set of "Safety Tips" for younger members that highlights the most important lessons for Internet safety (*i.e.*, they shouldn't post anything they wouldn't want the world to know; they should exercise caution when communicating with people they don't know; and they should avoid meeting strangers off line but, if they must, they should bring a friend or trusted adult). These tips appear on the MySpace registration page for any user who indicates he/she is under 18, and those users must affirmatively indicate that they've read these tips before they can register. *See* Attachment A. The tips have also been posted in the "mail" area for existing members of MySpace who are under 18. *See* Attachment B. In addition, MySpace will communicate safety tips and reminders periodically to under-18 users. Furthermore, now when a 14 or 15 year old changes their profile from private to public, a pop-up window is displayed again reiterating the new Safety Tips. *See* Attachment C.

We also revised the MySpace Safety Tips for parents and users that are available at the bottom of every page of MySpace to make them more clear and concise.<sup>2</sup> The Safety Tips for parents are designed to educate parents about the site and to help their children to make safe decisions about using online communities. They also encourage parents to talk to their kids about how they communicate with others and represent themselves on MySpace. Additionally, they provide parents with step-by-step instructions on how to remove their child's profile. They also provide links to software (including, as you requested, free software) to enable parents to monitor or block their child's use of the Internet, including blocking MySpace.

<sup>2</sup> The Safety Tips are available at <http://viewmorepics.myspace.com/misc/safetytips.html?z=1>; the Safety Tips for parents are available at <http://viewmorepics.myspace.com/misc/tipsForParents.html>.

HOGAN & HARTSON L.L.P.

The Honorable Richard Blumenthal  
 April 9, 2006  
 Page 3

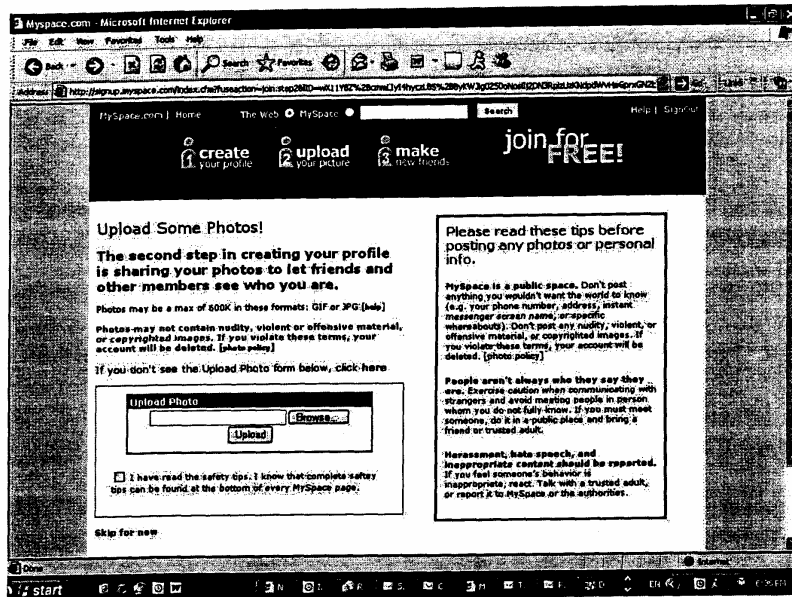
As you suggested, MySpace has also revised its Terms of Use (available at <http://viewmorepics.myspace.com/misc/terms.html?z=1>) to provide more specific details on the acceptable uses of MySpace. In response to another concern your staff expressed at our meeting, MySpace has blocked the ability to search or select the category "swingers" from any user under the age of 18. MySpace is categorizing online groups that contain adult content as "adult only," and thus limiting access to such groups to registered users over 18.

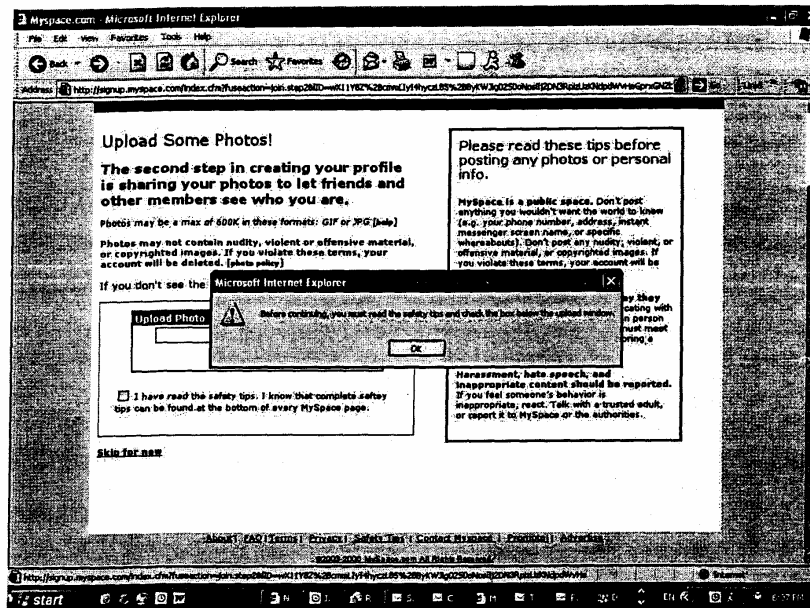
As you know, MySpace has created an Official Law Enforcement Officers Guide. This Guide has been distributed to every available law enforcement, state trooper, and Fraternal Order of Police association, NCMEC and its contacts, and substantially all law enforcement officers who ever contacted MySpace. MySpace continues to work closely with law enforcement on their requests for information, which have increased as a result of distributing the Guide. MySpace has a team of employees answering the dedicated law enforcement hotline number, 24 hours a day, 7 days a week.

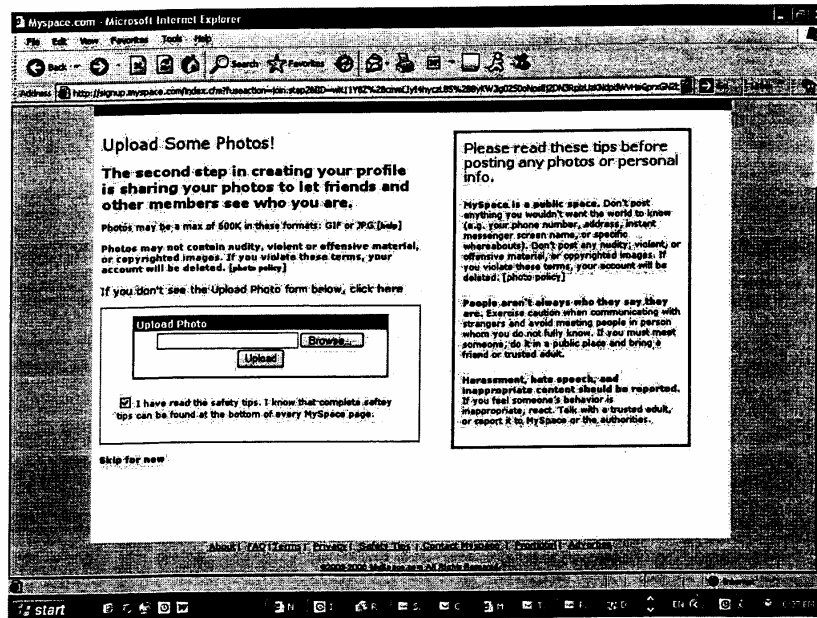
MySpace is planning a series of additional outreach programs to emphasize online safety in the age of social networking, including actively working with several advocacy and educational groups on promoting online safety. News Corporation has launched an extensive multi-media Public Service Announcement (PSA) campaign on Internet safety in conjunction with NCMEC and The Advertising Council. The PSAs will air on primetime on Fox broadcast and cable networks, radio, and across Fox Interactive Media's network of websites including MySpace, FoxSports.com, IGN.com, Fox.com, AmericanIdol.com, Rotten Tomatoes and AskMen. MySpace intends to work with other advocacy groups via multiple media outlets on future PSA campaigns.

MySpace is creating a curriculum to help law enforcement track suspicious behavior on the Internet, and educate the public. MySpace also plans to communicate with PTAs, schools, church or civic groups, and local organizations to educate teens and families on Internet safety.

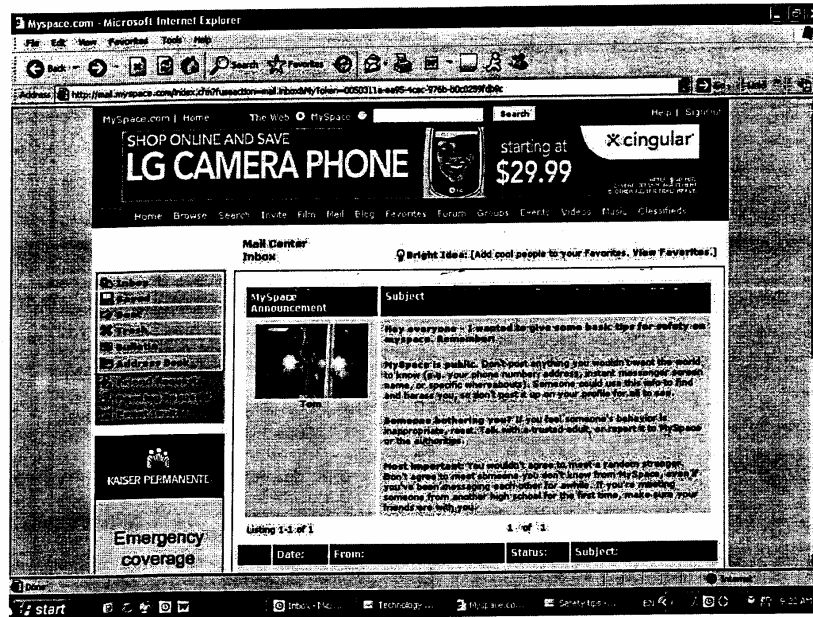
At our meeting we explained the difficulty of dealing with content that is not hosted by MySpace, but is rather "deeplinked" to our site by users. MySpace is attempting to find technological solutions to the issue of "deeplinked" images that do not meet MySpace's Terms of Use and Photo Policy. MySpace is currently in serious discussions with software providers to determine whether a solution is possible. In the meantime, MySpace has notified the two largest image hosting sites on MySpace that those sites must review the content they host and comply with MySpace's policies. MySpace is preparing Letters of Agreement for both sites that will memorialize these requirements; if the sites do not comply, MySpace is prepared to block access of those site(s).











03/26/2006 16:24 FAX

002

## State of Connecticut

RICHARD BLUMENTHAL  
ATTORNEY GENERAL



Hartford

March 20, 2006

Attorney Christine Varney  
Hogan & Hartson, LLP  
Columbia Square  
555 Thirteenth Street, NW  
Washington, D.C. 20004

Dear Ms. Varney:

I have appreciated your responding to my concerns about MySpace.com ("MySpace"), providing the opportunity to meet with you and your colleagues, including MySpace.com's Chief Executive Officer Chris DeWolfe, as well as our continuing discussions.

The preliminary steps outlined in your letter are a welcome start, but I am deeply concerned that they would leave children at risk from pornography and sexual predators and other potential problems. While our discussions have been encouraging, I ask MySpace to take certain specific practical steps to address immediately the most critical concerns identified by my office. These measures are technologically feasible, as well as consistent with your stated terms of service and your own explicit goal of prohibiting nudity and other offensive or inappropriate material from your website:

- Provide filtering software on the website that parents can download to block access to MySpace, as well as other websites that include sexually explicit material and other inappropriate content.
- Ban anyone under 16 from MySpace. If 14 and 15 year olds have access to any site, it should be separate and distinct. This new possible website should also ban children under the age of 14.
- Initiate a member login with age verification to regulate visitors viewing other member profiles, including pictures and access to group materials. Any access to adult content should be vigorously restricted to individuals 18 or older.
- Implement technology to ensure that 14 and 15 year olds are prohibited from changing their profile settings from private to public, and no photos or profiles of minors can be viewed by anyone older than 16 without parental consent.
- Increase staffing and employ additional filtering technology to effectively block nudity and sexually explicit images and other violations of MySpace terms of service and preclude people looking for sex from communicating or contacting

03/26/2008 16:24 FAX

003

children. MySpace should also do proactive manual searches of its site for material that violates its terms of service.

- Delete anyone who violates MySpace terms of service, and permanently ban a user from MySpace for continually posting prohibited deep links with pornography or other inappropriate material.
- Establish the new Security Director as an aggressive watchdog independent and separate from the corporate hierarchy reporting directly to the Board of Directors.
- Delete explicit reference to swingers as a browse term and groups or clubs identified as swingers or people seeking sex.
- Fully disclose in clear and conspicuous terms that MySpace contains explicit sexual content and users seeking sexual encounters, and prior use of the site by sexual predators to target minors.

Although new technology may be needed to fully protect children, much of it is already available. This site now exposes young people to a perilous cyber environment with people posting sexually explicit materials and looking for sexual relationships. In fact, children can still view pornographic images, links to X-rated websites, "clubs" involving adults seeking sexual encounters, and webcam sex for sale offers. I ask you to adopt my proposed steps immediately even as you develop new technology offering better protections.

I am prepared to continue our constructive discussions and ask that you contact my office. I welcome any other ideas you may have for advancing our shared goal of making MySpace a safe site for all. Again, thank you for taking the time to visit us and being responsive to our concerns. I look forward to making further progress in the coming days.

Sincerely,



RICHARD BLUMENTHAL

RB/pas

HOGAN & HARTSON  
L.L.P.

CHRISTINE A. VARNEY  
PARTNER  
(202) 637-6623  
CVARNEY@HHLLAW.COM

February 15, 2006

COLUMBIA SQUARE  
555 THIRTEENTH STREET, NW  
WASHINGTON, DC 20004-1109  
TEL (202) 637-6600  
FAX (202) 637-6910  
WWW.HHLLAW.COM

**CONFIDENTIAL - BY ELECTRONIC MAIL  
AND UNITED PARCEL SERVICE**

The Honorable Richard Blumenthal  
Office of the Attorney General  
55 Elm Street  
Hartford, CT 06106

**Re: MySpace Initiatives**

Dear General Blumenthal:

On behalf of MySpace.com ("MySpace"), thank you for the opportunity to meet with you and your staff on February 6, 2006. As you know, MySpace is committed to being the industry leader in social networking communities, and therefore, in addition to its current safety-related procedures, MySpace is developing several new safety initiatives.<sup>1</sup>

**MySpace's Current Safety Procedures**

MySpace's current procedures include providing a link on each page of MySpace.com to: (1) the Terms of Service, (2) the Privacy Policy, (3) Safety Tips, and (4) a link to "Contact MySpace," which presents an easy way for users to report "abuse" on the site including "underage users" and "inappropriate content." The MySpace Photo Policy prohibits posting photos that contain "nudity, pornography and sexually explicit images." MySpace removes from the site any photos it discovers that violate this policy, and provides a link for users to report offending photos.

MySpace is diligent in reviewing its site for inappropriate content. It devotes a significant portion of its staff time, energy, and money to addressing content, safety, and security issues on the site. Among other things, the staff attempts to review all photos and images that

<sup>1</sup> This letter and all enclosed documentary materials are and shall be treated as CONFIDENTIAL and be exempted from disclosure under the Connecticut Freedom of Information Act, Conn. Gen. Stat. § 1-210(b)(5), and all other applicable statutes and regulations.

HOGAN & HARTSON L.L.P.

The Honorable Richard Blumenthal  
February 15, 2006  
Page 2

are uploaded to the MySpace site and works to screen for compliance with the Terms of Service and Photo Policy. MySpace also encourages its users to notify it about content on the site that violates MySpace policies. At the bottom of each profile page there is a link to "Report Inappropriate Content," as well as "Contact MySpace" links throughout the site, where users can report any profile or other area of the site with questionable content. MySpace personnel investigate any report, and if an image on the site violates the Terms of Service, the Photo Policy or is deemed inappropriate, the image and possibly the entire profile will be deleted. MySpace staff will, as warranted by the circumstances, additionally investigate the user's friends to look for patterns and more inappropriate content.

As we explained to you at our February 6 meeting, despite our review efforts, inappropriate material may appear on MySpace through "deeplinks" to other sites. As we discussed, deeplinked images are not resident on the MySpace servers, but rather are provided to the site through another company's servers. MySpace has been in negotiations with the two largest image hosting sites used by MySpace members, and has demanded that they monitor the images uploaded to their sites in an effort to reduce objectionable third party-hosted content deeplinked to the MySpace site by members. Even though MySpace cannot review the deeplinked images as a matter of course due to technological limitations, it does have the "Report Inappropriate Content" mechanism for users to notify MySpace of such content. MySpace then reviews all reported images as part of the review process described above.

MySpace is constantly engaged with local police and investigators regarding user safety. MySpace has been praised for its cooperation with local, state and federal law enforcement agencies. Since its creation, MySpace has met with law enforcement officials throughout the country to solicit their viewpoints on how MySpace can enhance its cooperation with law enforcement and increase user security. MySpace has created streamlined procedures for law enforcement to submit subpoenas and other legal process to MySpace to obtain critical data that can be used to find and prosecute criminals. We have attached MySpace.com's Official Law Enforcement Officers Guide for your reference.

Any child pornography found on MySpace is immediately removed and reported to law enforcement. MySpace has worked with law enforcement to develop procedures that enhance the police's capability to monitor, gather evidence, and apprehend perpetrators. MySpace is committed to the vigorous prosecution of all purveyors of illegal material and provides both police and prosecutors all necessary support.

MySpace is very concerned about the safety of underage users on the site. The registration page requires prospective members to enter their exact birth date, and individuals who enter a date that does not meet the requisite age are not permitted to register. Once a user

HOGAN & HARTSON L.L.P.

The Honorable Richard Blumenthal  
February 15, 2006  
Page 3

enters an underage date, MySpace places a session cookie on their computer to prevent another registration attempt during the same browser session, *i.e.* preventing "back-buttoning."

If an individual is underage but enters a false birth date and is able to register for the website, there are still mechanisms in place to discover such underage users. MySpace has developed a search methodology to seek out such individuals, using over 1,000 search terms to alert the staff to a possible underage user on the site. The site is scanned for such terms, and the database of search terms is constantly updated to reflect changes in user behavior and terminology. All profiles which are identified by these scans as potentially belonging to an underage user are then individually reviewed by MySpace personnel. Whenever an underage user is discovered, the profile is deleted. Over 200,000 underage users have been deleted as a result of this scanning process. In addition, the MySpace customer support team sifts through profiles on the site to identify possible underage users that have been reported by MySpace members to MySpace.

In the event a registered user is between 14 and 17 years old, MySpace maintains extra safety mechanisms to protect them. Profiles of users who are 14 and 15 are automatically set to be private. This means that only the user's "friends" (that is, individuals that the user has affirmatively chosen to add to his or her "friends" list) will be able to view the profile. Additionally, only the user's friends will be able to send email messages or IM messages to the user, or add the user to a blog list. Users who are 14 and 15 years of age do have the option to opt out of the default privacy setting; however, their profile may still only be viewed by "friends" and users with a stated age of under 18 years. These privacy features are intended to prevent members who are 18 years of age or over from viewing a profile or sending an unsolicited message to users who are under 16.

#### New MySpace Safety Initiatives

In addition to these safety features, MySpace is considering several additional safety enhancements. First, MySpace has created a new, high-level Safety and Security Director position — reporting to the CEO — to create, oversee, and coordinate security operations across the site. This position will require a law enforcement background and will have the resources and support to implement the new and continuing safety initiatives.

#### Outreach Efforts

The MySpace Safety Tips for parents and teenagers are being revised in light of our meeting on Monday. MySpace will add to the Safety Tips an easy way for parents and schools to block access to the site on their computers if they choose. MySpace is also

HOGAN & HARTSON L.L.P.

The Honorable Richard Blumenthal  
February 15, 2006  
Page 4

considering additional ways to effectively communicate the prohibitions on inappropriate material currently contained in the Terms of Service. MySpace plans to communicate with PTAs, schools, church or civic groups, and local organizations to educate teens and families on Internet safety. MySpace plans to enhance its cooperation with law enforcement by distributing a Law Enforcement Guide on how to work with MySpace regarding subpoenas and requests for information.

MySpace is planning a series of additional outreach programs to emphasize online safety materials in the age of social networking. MySpace will work on these outreach programs individually, and hopefully in conjunction with other online community sites. MySpace intends to launch a multi-media Public Service Announcement (PSA) campaign on Internet safety via multiple media outlets in addition to online PSAs.

Dealing With Inappropriate Content on MySpace.com

As noted above, MySpace prohibits pornography or nudity on its site. As we discussed on February 6, it is more difficult to develop solutions to address the inappropriate material on MySpace that is not hosted on our server, but is deeplinked into the site from photo and video hosting services. MySpace is committed to working with the two largest photo hosting sites and numerous video hosting sites to set joint standards on appropriate materials on the MySpace site. If these photo and video hosting services do not meet these standards, MySpace is prepared to terminate their access to MySpace. MySpace has expedited its discussions with these services since our meeting.

MySpace appreciates your staff notifying it of some material that violates the MySpace Terms of Service. MySpace has removed all identified material (which were all served from third party photo serving sites), as well as researched associated friends. MySpace will also attempt to identify and investigate software that purports to serve pornography into the site. MySpace will block any software services whose purpose is to link pornography to the site.

Even with these technological solutions to blocking materials that violate the MySpace Terms of Service, there may be MySpace groups that engage in adult discussions that are constitutionally protected but are not appropriate for minors. For these adult-oriented groups, MySpace is looking at designating certain groups as "adult only." These groups would not be listed on the Groups List available on MySpace, and non-registrants and registered users under 18 would not be able to access or join adult only groups. For those users 18 and over, we will employ opt-in policies similar to those used by other leading online destinations to inform and protect our users.

HOGAN & HARTSON L.L.P.

The Honorable Richard Blumenthal  
February 15, 2006  
Page 5

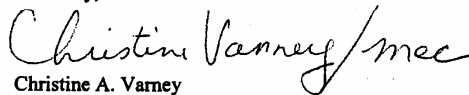
Protecting Younger Users

As described earlier, MySpace already has protections for users aged 14 and 15 by making their profile default to "private." If such a user attempts to change this setting, MySpace will now require a second confirmation, and will display to the user specific safety tips about the disclosure of personally identifiable information. In addition, MySpace will post an interstitial page to all registrants under the age of 18 so that they will read the tips prior to their completion of the registration. MySpace will also communicate safety tips and reminders periodically to those under-18 users. MySpace is investigating the technological feasibility of blocking search terms that could be used inappropriately to identify younger users. We are in the early stages of analyzing the potential to develop such a tool and its efficacy.

Your staff had inquired whether it would be possible to block the initial pictures of the "private" profiles from being viewed. After much discussion, MySpace believes that such a process would decrease the safety of its younger users. Given that the profiles are private, the initial picture acts as "caller id," identifying the requestor who is asking the recipient to add him/her as a "friend." Since no other information about the 14-15 year old is visible, the photo is a way of indicating to the teen who is contacting them. If the requestor's photo were masked, teenagers might be inclined to accept inappropriate invitations in order to see who had invited them to be a "friend." MySpace believes the likely acceptance of "blind" contacts creates an unacceptable safety risk for the very group of users it most wants to protect.

This is our beginning effort in what we consider to be an ongoing undertaking. Once again, we would welcome you and your staff to visit the MySpace facility in California. We believe such a visit may enhance your views as to our business and our commitment to running a clean, well-lit space for adults, young adults, and teenagers.

Sincerely,

  
Christine A. Varney

Enclosure





## XXXTORTION RAP FOR CYBER 'PERV'

By DAREH GREGORIAN

*June 19, 2006* — A 20-year-old Brooklyn man has been using the popular college-community Web site Facebook.com to con and extort coeds around the country, forcing them to turn over nude pictures of themselves and give him online companionship, officials said.

"Students think that because they're on a secure Web site like Facebook that they're safe from online predators," Manhattan District Attorney Robert Morgenthau said. "They're not."

Elvin Chaung is proof of that, the DA said - an alleged cyber-sicko who got over 50 women to send him nude photos and videos by posing online as one of their girlfriends. Investigators believe he tried the scam on hundreds of college students around the country.

"He was using identity theft and extortion to get naked pictures of 18- and 19-year-old women," said prosecutor Aaron Karczmer.

Most of Chaung's victims were his Hunter College schoolmates, but he also worked his manipulative magic on naive teens at over two dozen other colleges and universities, including Columbia, Karczmer said.

Sometimes the pictures weren't enough. On one occasion, he instant messaged a victim who realized she'd been conned into sending him racy pictures and threatened to humiliate her unless she continued "talking" to him, Karczmer said.

"As of now, I haven't done anything with them. Don't make me change my mind. I just want to chat . . . I want to get to know u more. Ur hotttt," Chaung - or "OneSweetgurlie" - wrote in one exchange, court records show.

If "I were to lose contact wit u I mite want to send the pics all over the internet. As long as we can chat and be friends the pics are safe."

Chaung, who lives with his parents in Ditmas Park, declined to comment. He's free on bail after being arrested and charged with identity theft, computer trespass and tampering, coercion and grand larceny.

In a recent hearing before Manhattan Criminal Court Judge Abraham Clott, Karczmer said Chaung has been working his scams since this past fall, using his Facebook account as a key to opening doors to coeds around the country.

Facebook is a popular online network that is aimed primarily at college students. It allows people with a college e-mail address to start their own Web pages, post pictures and talk online with friends, and allows them special access to other schoolmates' pages.

Chaung allegedly used his Facebook account to "case" female students, watching their pages to find out who their friends were and whatever he could about their backgrounds.

First, he'd claim to be an old high-school pal or a Facebook friend, using a new instant-messaging account because of "computer problems."

"I been IMin, textin, emaling callin everyone I know - EVERYONE I could think up of," "she" explained, saying "she" would've called but her cellphone was dead, records show.

Chaung would then say he was in big trouble with his photo or art professor and desperately needed pictures e-mailed to him, the records show. He said if he didn't get pictures for his "project," he would flunk the class and lose a \$2,000 scholarship.

After getting his victim to send a regular picture, he would then push for a bikini or lingerie shot, and then a nude shot, prosecutors said.

If the victim would balk at sending the nude photo, he'd threaten to plaster the bikini or lingerie shots around their schools unless they complied, records show.

Chaung told investigators the threats worked "approximately 10 percent of the time," court papers say.

In at least one instance, he carried out a threat, filings say.

He doctored a lingerie shot of a woman to make it look like she was naked and posted the pic on her friend's page, court papers say.

Anyone with information on the case is asked to call the Manhattan DA's identity-theft hot line at (212) 335-9600.

Chaung faces 21/2 to seven years in prison if convicted.

*Additional reporting by Tatiana Deligiannakis and Kenneth Kobel*

*dareh.gregorian@nypost.com*

[Click here to view Dot-con job graphic](#)

[Home](#)

---

NEW YORK POST is a registered trademark of NYP Holdings, Inc. NYPOST.COM, NYPOSTONLINE.COM, and NEWYORKPOST.COM are trademarks of NYP Holdings, Inc. Copyright 2006 NYP Holdings, Inc. All rights reserved.

**facebook**

**Welcome to Facebook.**

---

## facebook

### What is Facebook?

---

Facebook is a social utility that allows people to share information with their real world community

What is important to us:

- User Control: people should have control over their information
- Authenticity: ability to interact with others as themselves
- Accessibility: Facebook is becoming part of peoples' daily lives

Mission:

Provide people with the information that matters to them most

## facebook

### How does it work?

- Users are required to validate identity
  - College: school issued .edu email address
  - High School: school issued email address or invited by validated member
  - Work Networks: company or organization issued .com/.net/.org
- Users join a primary community
  - College, high school, company or organization
  - Profile views are by default restricted to those within validated communities
  - Facebook Groups & Events provide additional affinities
- Facebook is a core part of millions of young peoples' lives
  - Authentication and connection with real world community leads to deeper bonds and trust

## Four Levels of Protection

- **Initial Authentication:**
  - Restriction to validated email addresses means both confirmation of actual membership in particular communities and connection to real identity
  - Retains social norms and fosters sense of accountability, deterring misuse
- **Segmented Communities**
  - Requirement of validation in communities means high school users (especially) can easily identify who doesn't belong
  - Built-in Neighborhood Watch
- **Innovative Privacy Controls & Technical Protections**
  - Users have extensive power to decide who can see their profile
- **Outstanding Customer Service Staff and Cooperation with Law Enforcement**
  - 20+ experts on the site (recent college graduates) headed by the former worldwide director of customer support for Palm Computing
  - Specialized investigations staff within Customer Service
  - CPO and General Counsel work directly with law enforcement on rare problems

Internal and confidential January 2006 data

**FOR IMMEDIATE RELEASE****MYSPACE EXPANDS SAFETY AND SECURITY PRODUCT  
FEATURES TO HEIGHTEN ONLINE SAFETY FOR MEMBERS****Leading Social Networking Site to Increase Protection for 14-15 Year Old  
Members; Adds Ability for Members to Set Profile to Private**

LOS ANGELES—June 21, 2006—MySpace.com, the leading social networking and lifestyle portal, announced today new safety and security features designed to offer increased safety to its growing community of members. These additional safety features include heightened security for 14–15 year old members, new options for privacy settings for all members, and restrictions on ad placements to younger users.

Directing all MySpace's safety and security policies is newly appointed MySpace Chief Security Officer, Hemanshu Nigam, a former Federal prosecutor against Internet child exploitation for the U.S. Department of Justice.

"With social networking becoming a mainstream platform for millions of people to connect with one another and express themselves, MySpace is committed to innovating new product features to heighten online safety, particularly in the area of 14 to 15 year olds," said Nigam. "In addition to technology innovation, MySpace remains dedicated to a multi-pronged approach that also involves education and collaboration with law enforcement, teachers, parents and members."

MySpace's new enhanced safety features include:

- **Heightened Security Settings for 14 -15 Year Olds:** Furthering efforts to create a well-lit place for teens to connect and communicate online, MySpace will now protect 14 and 15 year olds from contact from strangers, who are over 18 years old. This new feature requires all 18+ year old members to know either the email address or first and last name of members who are under 16 years old to connect.
- **Full Privacy Settings for All Members:** MySpace members of any age have the option to set their profiles to private, allowing only friends within their private network to view detailed information such as personal interests and friends. In addition, MySpace members have the option to set their profile to restrict contact to members within their own age group.
- **Age Appropriate Ad Placements:** In an additional move to safeguard and enhance members' experience, MySpace is improving advertising targeting throughout the site based on age appropriateness. MySpace will engage in targeted online ad placements in order to promote safe Internet behavior.

"We know that children can benefit greatly from being online," said Ernie Allen, President and CEO of the National Center for Missing & Exploited Children (NCMEC).



Jim E. Fogarty  
Attorney General  
State of California

700 California Street  
San Francisco, CA 94104-3100  
Telephone: (415) 773-3300  
www.ca.gov/ag

March 24, 2006

Chris DeVolf, CEO  
MySpace.com  
1333 2nd Street  
Santa Monica, CA 90401

Dear Mr. DeVolf:

I am increasingly concerned by reports that young children using MySpace.com have been victims of harassment, sexual solicitation, and even sexual abuse. This incident is currently under investigation by the Alameda County Police Department involving the alleged rape of a 14-year-old Ohio student by an adult male who met her on your Web site. Although social networking sites can be a fun way to connect with friends and family, I am concerned that your current operating policies may put children at risk.

Over the last several months, my office and local law enforcement have received complaints from parents regarding the type of information minors can access on your site. A simple search on your site demonstrates that children can easily access a range of inappropriate material, such as pornographic images, ads for sexual profiles, obscene language and various references to the use of illegal substances. This material is in direct conflict with paragraph five of your "Terms of Use Agreement," which states, "a profile may not include the following items: photographs containing nudity, or obscene, lewd, excessively violent, harassing, sexually explicit or otherwise objectionable subject matter."

To address these concerns, I ask that you consider the following actions to safeguard children against potential abuse and exploitation. My office believes these enhancements would be in the best interest of all affected parties.

EXHIBIT

B



DeWolfe, Chris  
March 24, 2006  
Page 2

1. Increase the minimum user age from 14 to 16 and prohibit children from accessing the profile of another user.
2. Explicitly state in the Terms of Use Agreement and during registration that Myspace contains sexually explicit content and that users have an obligation of privacy in regards to information posted on Myspace.com.
3. Require that all new users must verify their email address during the registration process. Upon successful completion of the registration process, a brochure describing the site and the Terms of Use Agreement should be sent to the email address.
4. Place a "Report this profile" button on every user's profile.
5. Increase the company's ability to identify, remove, and block the violation of Myspace policies by expanding the use of filtering technology.
6. Implement a zero tolerance policy regarding the violation of the Terms of Use Agreement. Members violating the policy should be permanently barred from the site and their profiles should be taken down from the system.
7. Establish an independent board of community standards to proactively dealing with privacy and security concerns.
8. Prohibit minors from accessing groups, clubs, or profiles that contain adult content.

Although the convenience of the internet may be a gateway to infinite information, it can also be fraught with pitfalls that may be dangerous to an unsuspecting user. Under its current conceptualization, Myspace increases youth exposure to inappropriate material, placing them at a higher risk of victimization. It is my hope that you will immediately move to implement the recommendations listed above.

If you have any questions or concerns, please do not hesitate to contact me.

Very truly yours,

  
Chris DeWolfe  
Ohio Attorney General

Attorney Christine Varney  
Hogan & Hanson, LLP  
Columbia Square  
555 Thirtieth Street, N.W.  
Washington, D.C. 20001

Dear Mr. Varney:

I have appreciated your responding to my concerns about Myspace, Inc. ("Myspace") providing the opportunity for users to post and upload pictures, videos, and other content. Executive Officer Chad C. Brown, as well as others in the Myspace organization,

The preliminary steps outlined in your letter to me, dated March 21, 2007, have been taken. I am concerned that they will not be sufficient to protect the privacy and security of my children and other potential problems. While I do appreciate the steps you have taken, I am concerned that certain specific practical steps, which I highlighted in my letter to you, dated March 21, 2007, have not been taken. These measures are common to all of the social networking services that I use, and I am of service and your own explicit list of prohibited items and content, and I am concerned that material from your website.

- Provide all users with a copy of the list of prohibited items and content, and ensure that all users have access to Myspace's terms of service, which state that such prohibited material is not to be posted or uploaded.
- Ban anyone under 18 from Myspace. Under 18 year olds must be able to see if it should be parents and others. This may pose a problem for children under the age of 18.
- Initiate a member login with age verification so anyone viewing a user's member profile, including pictures and access to group material, can see if it should be parents and others. This may pose a problem for children under the age of 18.
- Implement technology to ensure that 18 and 15 year olds are prohibited from changing their profile settings from private to public, and to photos of profiles of minors can be viewed by anyone other than 18 without parental consent.
- Increase staffing and employ additional filtering technology to effectively block nudity and sexually explicit things and other violations of Myspace terms of service and preclude people looking for sex from communicating or contacting.



children. In Sweden, nearly 90% of children remain in their family of origin, and the majority of these children are raised in two-parent families. In the United States, 75% of children remain in their family of origin, but 25% of these children are raised in single-parent families. In the United Kingdom, 60% of children remain in their family of origin, but 40% of these children are raised in single-parent families. In the United States, 25% of children are raised in single-parent families, and 75% of these children are raised in two-parent families. In the United Kingdom, 40% of children are raised in single-parent families, and 60% of these children are raised in two-parent families. In the United States, 75% of children are raised in two-parent families, and 25% of these children are raised in single-parent families. In the United Kingdom, 60% of children are raised in two-parent families, and 40% of these children are raised in single-parent families.

Although new technologies have increased the availability of information, the information is not always available. Thus, in a new study, researchers have found that posting sexually explicit information on the Internet is associated with a lower view of pornography, less sexual satisfaction, and less sexual confidence, and women are less likely to have a sexual partner. Even as our lives have become more technologically sophisticated,

I am prepared to defend my position in court, if you like. I will come any day of the week, at any hour, to discuss my position online. My space is available for all to visit, and I will explain my position to all who wish to hear. I have no agenda, and I have no intention of converting anyone to our religion. I have no intention of making money. I am a Christian, and I

511

**RICHARD L. BENTON**

**RESEARCH**

## SOCIETY

By JULIE RAWE

**A**S FIRST DATES GO, THIS ONE WASN'T terribly original: dinner and a movie, followed by a lot of time in a parked car. The two teenagers, who in mid-May chowed down at a Whataburger in Austin, Texas, before going to see *Mission: Impossible III*, certainly weren't the first guy and girl to meet on MySpace. And they are far from the only members who have fibbed on the hugely popular hangout site—her profile bumped her age up a year while he allegedly posed as a high school senior. But what makes the Texas encounter unique is that the 19-year-old guy, Pete Solis, got arrested for having sex with a minor, and the 14-year-old girl, whose name has not been released, sued MySpace for failing to protect underage users from online predators.

The lawsuit, which is seeking \$30 mil-

lions in damages, comes on the heels of another headline grabber in which a 16-year-old honors student in Michigan flew as far as Jordan before her parents realized she was planning to rendezvous with—and marry—a West Bank man she had met on MySpace. With countless parents now wondering what kind of liaisons their kids are forging online, law-enforcement agencies and elected officials have begun to step up their efforts to get teen-laden networking sites to improve their safety measures. Attorneys general of 22 states have called on the sites to set more boundaries for interactions between users, and this week Congress is scheduled to hold two days of hearings on how to make the Internet safe for kids. Executives who operate these sites acknowledge the concerns but say they lack the ability to monitor millions of daily exchanges and can't even verify members' ages. "There is no technology or national system that exists that allows us or any Internet company to verify the identity of people online," says Hemanshu Nigam, MySpace's chief security officer.

For parents who have only a passing knowledge of MySpace, let alone the ever multiplying horde of competitors like Xanga, Facebook and Bebo, it may be hard to understand why kids flock to these sites and how they can be more dangerous than old-school chat rooms. The reason: in chat rooms, predators have to engage in conversation to get to know people. But on sites like MySpace, they can access gobs of information by reading users' profiles, which tend to include photos as well as blog entries and bantering with friends. "It's totally addictive," Hannah Kranz, 16, says of MySpace. "My cousin gave it up for Lent." Kranz, who lives in Ferndale, Wash., says she interacts only with users she already knows offline and feels secure because, as she explained to her parents, the site lets her accept or deny an invitation to be someone's friend—and thus control who accesses the full content of her profile. Some kids, however, eager to appear popular (MySpace tal-

## A Site in the Hot Seat



# MYSPEACE?

**Social-networking sites are all the rage with kids. Now a lawsuit accuses the most popular one of not doing enough to protect them from predators**

lies the number of friends each user has), post bulletins asking everyone to befriend them, a practice, Kranz says, that is known as "whoring yourself." With nearly 85 million MySpace users and free accounts being opened at the blistering pace of more than 250,000 a day, it's difficult to keep track of who is responding to those solicitations.

The FBI says arrests of Internet predators more than tripled from 2001, to 1,649 last year, and there have already been more than 1,000 arrests so far this year. Experts note that even with this increase—attributed in part to more resources being thrown at the problem—the number of online-predator arrests is still small compared with the overall arrests for sexual assaults against minors, which in 2000 was estimated to be 66,000 nationwide. Even so, that same year a survey conducted by the Crimes Against Children Research Center at the University of New Hampshire found that nearly 1 in 5 kids had received unwanted sexual solicitations over the Internet. And a March 2006 survey partly funded by the National Center for Missing & Exploited Children reported that 14% of

teens have actually met face to face with someone they had known only through the Internet. Lately, there has been news almost every other day of someone getting busted for having sex with a kid he met on MySpace. And the newsmagazine show *Dateline* has turned online sting operations into the hit series "To Catch a Predator," which has led to the arrests of at least 96 men.

MySpace has long had certain protective measures in place, such as a prohibition against posting last names, street addresses and phone numbers. But the suit filed last week against Solis, MySpace and its parent company, News Corp., which bought the site last summer for \$580 million in cash, notes that even though new members have to submit their name, gender and date of birth, "none of this has to be true." Indeed, while MySpace maintains that it prohibits anyone under 14 from joining the site and anyone 18 and older from viewing profiles of those 17 and under, Solis and the girl both managed to thwart these restrictions. Solis, who has no prior criminal record, says he hopes the charges

Illustration for TIME by Matt Mahurin

35

## SOCIETY

against him get reduced to injuring a child.

After the lawsuit was filed, MySpace, which removes pornography as well as obviously underage users from its site, announced additional restrictions, including preventing members under 16 from being contacted by users 18 and older unless they know the kids' full names or e-mail addresses. That, of course, won't keep out (or keep safe) people who lie about their age. "The big question," says Randy Barnett, a contracts and cyberlaw professor at Georgetown University, "is what could MySpace do to effectively prevent the misuse of its website, short of not providing the service at all?"

Several state prosecutors have suggestions. Massachusetts wants the minimum age on social-networking sites raised to 18. North Carolina is calling for a 24-hour waiting period to allow screeners to review changes to users' profiles, which would make these dynamic sites a real drag. Connecticut, meanwhile, has talked to Defense Department vendors to see what technology is available to screen content for key terms that might raise a red flag. The one issue all the states seem to agree on is the need to verify users' ages.

Industry and government officials discussed this proposal and others at a social-networking summit last week in Washington. But there is no easy solution when it comes to confirming information about teens, only some of whom have credit cards or a driver's license. Industry watchers say Social Security numbers may not be a cure-all either, in part because of the global nature of these sites—the biggest of which, MySpace, said last week it is expanding into 11 other countries. Connecticut attorney general Richard Blumenthal didn't accept all the naysaying: "Don't tell me it can't be done. If we can put a man on the moon, we can verify age." All 50 state prosecutors are scheduled to meet this week to discuss social networking, and at least one of them is actively looking into filing large-scale consumer-protection suits, according to a source who works with that attorney general.

The social-networking sites are hoping to avoid such an outcome, in part by urging parents to be more proactive and users to do more self-policing. "That's the real story here," says John Hiler, CEO of Xanga, whose 27 million users often report questionable content. "There are a lot of skeptics who say things like 'Youth can't participate in self-policing.' I think the jury is still out on that." In the end, they may be their own best defense. —With reporting by Melissa August, Brian Bennett and Tracy Schmidt/Washington, Hilary Hyton/Austin and Jeffrey Resner/Los Angeles

36

## VIEWPOINT

Robert Putnam

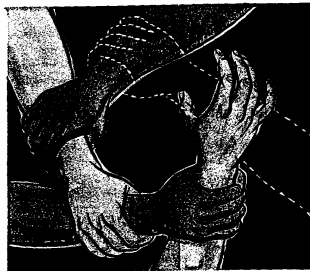
## You Gotta Have Friends

A study finds that Americans are getting lonelier

**A**mericans are more socially isolated today than we were barely two decades ago. The latest evidence of that comes from a topflight team of sociologists who, after comparing national surveys in 1985 and 2004, report a one-third drop in the number of people with whom the average American can discuss "important matters."

That startling report raises four questions: 1) Is it true? 2) Why has it happened? 3) Does it really matter? And 4) if so, what can we do about it?

I confess a personal stake in the first question. Six years ago in a book I wrote called *Bowling Alone*, I argued that the fabric of American communities has frayed badly since the mid-1960s. I traced plummeting membership in PTAs, unions and clubs of all sorts; long-term declines in blood donations, card games and charity; and drops of 40% to 60% in dinner parties, civic meetings, family suppers, picnics and, yes, league bowling.



Just as the debate about global warming began with controversial claims made by a few iconoclasts, so too were many sociologists skeptical of my findings about lonely bowlers. No complex issue is ever settled by a single study. Advancing the global warming argument has required decades of research, and it may take another decade to convince the final doubters that social connectivity in the U.S. has, in fact, disintegrated. But that latest study is an important milestone.

Ironically, the authors began their work deeply skeptical about my argument. To their credit, when the unexpected results came back, they scratched their heads, kicked the tires really hard to ensure there was no mistake and last week reported their findings in a paper aptly called "Social Isolation in America."

Why this sharp increase in social isolation? Both the new study and mine found sharp generational differences—baby boomers are more socially marooned than their parents, and the boomers' kids are lonelier still. Is it because of two-career families? Ethnic diversity? The Internet? Suburban sprawl? Everyone has a favorite culprit. Mine is TV, but the jury is still out.

Does it really matter? As a friend said, "So what if the average American now has two close friends, not three? Two is plenty." But that's exactly like saying, "If global temperatures rise from 65°F to 70°F, I wouldn't even notice." That's fine, as long as you ignore the indirect effects, like mega-hurricanes in the Gulf.

Social isolation has many well-documented side effects. Kids fail to thrive. Crime rises. Politics coarsens. Generosity shrivels. Death comes sooner (social isolation is as big a risk factor for premature death as smoking). Well-connected people live longer, happier lives, even if they have to forgo a new Lexus to spend time with friends.

So what can be done? Unlike global warming, we can solve this problem fairly easily by simply getting more involved in our communities and spending more time with family and friends. Family-friendly workplaces would help too. Reaching out to a neighbor or connecting with a long-lost pal—even having a picnic or two—could just save your life.

Putnam is a professor at Harvard University and the author of *Bowling Alone*

TIME, JULY 3, 2006

[Whereupon, at 5:21 p.m., the subcommittee was adjourned.]

